TASK ORDER

47QFCA20F0010
Modification P00052

Border Enforcement Applications for Government Leading-Edge Information Technology (IT) (BEAGLE)

in support of:

Department of Homeland Security (DHS) Customs and Border Protection (CBP) Office of Information & Technology (OIT) Border Enforcement Management Systems Directorate (BEMSD)

Issued to:
CACI Inc. - Federal
14370 Newbrook Drive
Chantilly, VA 21051

Awarded under GSA Alliant 2 Government-wide
Acquisition Contract 47QTCK18D0009
Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

November 05, 2019
FEDSIM Project Number HS01037

B.1 GENERAL

The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Basic Contract, under which the resulting TO will be placed. An acronym listing to support this Task Order Request (TOR) is included in Section J, Attachment B.

B.2 CONTRACT ACCESS FEE (CAF)

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a CAF. In accordance with the Alliant 2 base contract, the CAF shall be 0.75 percent of the total TO value with a cap of $100,000 per year per order (when order is in excess of $13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO Award (TOA).

B.3 ORDER TYPES

The contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for mandatory CLINs 0001, 1001, 2001, 3001, 4001, and 0007; CPAF for optional CLINs 0002, 1002, 2002, 3002, and 4002; and a Not-to-Exceed (NTE) basis for CLINs 0003, 1003, 2003, 3003, 4003, 0004, 1004, 2004, 3004, 4004, 0005, 1005, 2005, 3005, 4005, 0006, 1006, 2006, 3006, 4006.

B.4 SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 50 miles from duty station as defined in Section F.2. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CAF	Contract Access Fee
CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
NTE	Not-to-Exceed
ODC	Other Direct Cost

B.4.1 BASE PERIOD:

MANDATORY CPAF LABOR CLIN

Only award fee may be proposed; base fee shall not be proposed.

CLIN	Description	Cost	Award Fee	Total CPAF
0001	Labor (Tasks 1 - 8)	(b) (4)		

OPTIONAL TASK 9 LABOR CPAF CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
0002	Labor (Task 9)	(b) (4)		

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
0003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$ 1,000,000
0004	Tools Including Indirect Handling Rate (b) (4)	NTE	$ 25,000,000
0005	ODCs Including Indirect Handling Rate (b) (4)	NTE	$ 5,000,000

CAF

CLIN	Description		Total Ceiling Price
0006	CAF	NTE	$ 100,000

TOTAL CEILING BASE PERIOD CLINs: $ 185,582,061

B.4.2 FIRST OPTION PERIOD

MANDATORY CPAF LABOR CLIN

Only award fee may be proposed; base fee shall not be proposed.

CLIN	Description	Cost	Award Fee	Total CPAF
1001	Labor (Tasks 1 - 8)	(b) (4)		

OPTIONAL TASK 9 LABOR CPAF CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
1002	Labor (Task 9)	(b) (4)		

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
1003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$ 1,000,000
1004	Tools Including Indirect Handling Rate (b) (4)	NTE	$ 25,000,000
1005	ODCs Including Indirect Handling Rate (b) (4)	NTE	$ 5,000,000

CAF

CLIN	Description		Total Ceiling Price
1006	CAF	NTE	$ 100,000

TOTAL CEILING FIRST OPTION PERIOD CLINs: $ 233,588,398

B.4.3 SECOND OPTION PERIOD

MANDATORY CPAF LABOR CLIN

Only award fee may be proposed; base fee shall not be proposed.

CLIN	Description	Cost	Award Fee	Total CPAF
2001	Labor (Tasks 1 - 8)	(b) (4)		

OPTIONAL TASK 9 LABOR CPAF CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
2002	Labor (Task 9)	(b) (4)		

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
2003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$ 1,000,000
2004	Tools Including Indirect Handling Rate (b) (4)	NTE	$ 25,000,000
2005	ODCs Including Indirect Handling Rate (b) (4)	NTE	$ 5,000,000

CAF

CLIN	Description		Total Ceiling Price
2006	CAF	NTE	$ 100,000

TOTAL CEILING SECOND OPTION PERIOD CLINs: $ 236,281,745

B.4.4 THIRD OPTION PERIOD

MANDATORY CPAF LABOR CLIN

Only award fee may be proposed; base fee shall not be proposed.

CLIN	Description	Cost	Award Fee	Total CPAF
3001	Labor (Tasks 1 - 8)	(b) (4)		

OPTIONAL TASK 9 LABOR CPAF CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
3002	Labor (Task 9)	(b) (4)		

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
3003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
3004	Tools Including Indirect Handling Rate (b) (4)	NTE	
3005	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CAF

CLIN	Description		Total Ceiling Price
3006	CAF	NTE	(b) (4)

TOTAL CEILING THIRD OPTION PERIOD CLINs: $ (b) (4)

B.4.5 FOURTH OPTION PERIOD

MANDATORY CPAF LABOR CLIN

Only award fee may be proposed; base fee shall not be proposed.

CLIN	Description	Cost	Award Fee	Total CPAF
4001	Labor (Tasks 1 - 8)	(b) (4)		

OPTIONAL TASK 9 LABOR CPAF CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
4002	Labor (Task 9)	(b) (4)		

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
4003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
4004	Tools Including Indirect Handling Rate (b) (4)	NTE	
4005	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CAF

CLIN	Description		Total Ceiling Price
4006	CAF	NTE	(b) (4)

TOTAL CEILING FOURTH OPTION PERIOD CLINs: $ (b) (4)

B.4.6 TRANSITION-OUT SEVERABLE LABOR CLIN (SIX MONTHS):

Only award fee may be proposed; base fee shall not be proposed.

CLIN	Description	Cost	Award Fee	Total CPAF
0007	Transition-Out Labor (Task C.5.2.2)	(b) (4)		

TOTAL CEILING TRANSITION-OUT SEVERABLE LABOR CLIN: (b) (4)

GRAND TOTAL CEILING ALL CLINs: **$ $1,144,842,223**

B.5 SECTION B TABLES

B.5.1 INDIRECT/MATERIAL HANDLING RATE

Long-Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the basic contract does not prohibit the application of indirect rate(s) on these costs.

a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.5.2 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing Alliant 2 labor categories.

B.6 INCREMENTAL FUNDING

B.6.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of **$411,136,905** for CLINs **0001, 0003, 0004, 0006, 1001, 1003, 1004, 1006, 2001, 2002, 2003, 2004, and 2006** is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through **July 31, 2022**, unless otherwise noted in Section B. The TO may be modified to add funds incrementally up to the maximum of **$1,144,842,223** over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart for CPAF

See Section J, Attachment C - Incremental Funding Chart (Excel Spreadsheet).

B.7 AWARD FEE

The Award Fee Determination Plan (AFDP) establishes award fee. See Section J, Attachment D - Award Fee Determination Plan (Word document).

C.1 BACKGROUND

The Bureau of Customs and Border Protection (CBP) is a component of the Department of Homeland Security (DHS). The priority mission of CBP is to prevent terrorists and terrorist weapons from entering the United States (U.S.). This important mission calls for improved security at America's borders and ports of entry as well as for extending the zone of security beyond physical borders so that American borders are the last line of defense, not the first. CBP is also responsible for apprehending individuals attempting to enter the U.S. illegally; stemming the flow of illegal drugs and other contraband; protecting the U.S. agricultural and economic interests from harmful pests and diseases; protecting American businesses from theft of intellectual property; regulating and facilitating international trade; collecting import duties; and enforcing U.S. trade laws.

C.1.1 PURPOSE

Under the Border Enforcement Applications for Government Leading-Edge Information Technology (IT) (BEAGLE) requirement, the Border Enforcement Management Systems Directorate (BEMSD) is seeking to obtain greater integration, automation, innovation, cost savings, and efficiencies within its portfolio of applications through the use of Agile-based methodologies, integrated testing, and transformative processes to support current and future requirements. This will include standard architectures, advanced analytics, and Business Intelligence as well as a SecDevOps path to production and instantiation of mature, industry- and performance-based best practices. Legacy applications must continue to be operated and maintained with high levels of application availability while enhancements to and/or modernization of existing applications or the development of new solutions are addressed.

C.1.2 AGENCY MISSION

The primary customer of BEAGLE is CBP's Office of Information and Technology (OIT) and specifically, BEMSD within OIT. BEMSD's role is to plan, provide, develop, and sustain applications, tools, and services that perform a variety of capabilities that enable the overall CBP mission. These applications include asset and real property management, border enforcement, agent safety and tracking, surveillance asset activity, capture, and communication, mission planning and forecasting, case management, geospatial mapping, incident response and reporting, tracking of vehicles and personnel, firearms tracking and credentialing, and financial management. These applications enable rapid decision making, allowing CBP personnel to anticipate and respond to threats.

C.2 SCOPE

The scope of this effort is to provide a full range of IT-related services and technical solutions that encompass application administration services, property accountability, asset management, operations, configuration management, change management, incident management, cloud migration, capability backlog remediation, knowledge management, training, project management, problem management, release management, security and audit management, testing, quality assurance, and sustainment requirements of the CBP OIT BEMSD agency mission. Contractor is required to perform operational maintenance and systems development services for BEMSD through standardized industry best practices (e.g., IT Service Management (ITSM)-based procedures). BEMSD serves as the solutions owner and interface between the

contractor and CBP and other external customer offices; as such, all discussions regarding BEMSD systems with CBP customers must include the appropriate BEMSD representatives.

C.3 CURRENT INFORMATION TECHNOLOGY/NETWORK ENVIRONMENT

BEMSD's core competency and primary objective is to support CBP's mission. Aging IT infrastructure and applications have resulted in reduced application availability and have limited opportunities to innovate and deliver cutting-edge technology to address ever-changing mission needs. Currently, BEMSD operates a high volume of legacy mission-oriented systems with fundamental challenges, including lack of resiliency and Disaster Recovery (DR) that cannot be adequately addressed without modernization. Applications and capabilities exist in siloed architectural structures.

BEMSD also faces a large amount of technical debt in its legacy, mission-critical/-essential systems, resulting in slower, less scalable systems and architecture. Rapidly building and architecting new solutions for evolving operational needs has led to the majority of this technical debt. To use resources more effectively, the contractor shall develop new solutions according to a strategic vision, as well as scaling pilot capabilities to become long-term solutions. Technical debt has constrained BEMSD's ability to provide new capabilities (e.g., cloud, mobility), remain compliant with cybersecurity policies, and reduce outage risk to mission-oriented systems.

C.4 OBJECTIVES

Objectives of the BEAGLE TO include the following:

a. Mission Support
b. SecDevOps
c. Cloud Migration
d. Modernization
e. Innovation
f. Reduction of Operations and Maintenance (O&M) Spending

C.4.1 MISSION SUPPORT

BEMSD's work supports the missions of CBP and a broad range of stakeholders, both within CBP and externally. BEMSD supports critical components of CBP's overall mission, including areas that directly impact agent and officer safety, impact the flow of trade and related finances, and provide communications to internal and external stakeholders. Some of BEMSD's services and systems support other DHS and law enforcement community stakeholders and missions, including Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), the Federal Bureau of Investigation (FBI), and State and Local law enforcement. Some of these stakeholders and missions require support 24 hours a day, seven days a week, and 365 days a year (24x7x365), in particular, those supporting agent and officer safety as well as critical chain of command communications.

BEMSD follows a CBP-wide designation for systems and applications (i.e., Mission Critical System, Mission Essential System, and Mission Relevant System). These designations drive the level of support and response times required in support of the respective category of system or application.

In addition, BEMSD provides full lifecycle development services for new functionality, new capabilities, and new systems. These services cannot adversely impact the performance and availability of, or support to existing systems. BEMSD requires well-coordinated support to ensure seamless services, even as new or unanticipated requirements may present themselves. BEMSD is seeking an approach that prioritizes mission support in appropriate balance with the technical objectives of this TO (e.g., SecDevOps, cloud migration, modernization, innovation, and O&M expense reduction) in order to provide timely, affordable support to end users' most critical needs.

C.4.2 SECDEVOPS

BEMSD's clients and end users represent a broad range of front-line CBP and external users, and BEMSD's systems support important mission functions. As such, there is a need to deliver new useable functionality and new systems and applications as quickly as possible, and ensure the existing systems are reliably available while buying down technical debt as efficiently and effectively as possible. While not quantified in a consistent manner across the portfolio, technical debt is most frequently defined as the additional overhead on applications caused by delayed modernization to existing solutions, which leads to more manual operations being needed to apply basic O&M features (ex. patching, upgrades). A tailored, consistent, and adhered-to SecDevOps approach is one important aspect of delivering this needed support.

BEMSD seeks to institutionalize coordinated and consistent SecDevOps practices, with support that provides best practices aligned with mature Agile-enabled organizations. Today, BEMSD employs a combination of approaches in its development and maintenance activities, with SecDevOps in some form being implemented across roughly 20% of the BEMSD portfolio, and only a low number of automation workflows defined or implemented. As BEMSD also seeks increased efficiencies, reductions in the cost of O&M, and improved accuracy and timeliness in the delivery of functionality, BEMSD is looking for SecDevOps solutions that support these important goals.

C.4.3 CLOUD MIGRATION

BEMSD is transitioning from a monolithic, system-based architecture to one focused on microservices. BEMSD is seeking to smartly migrate applications to the cloud in order to better support mission applications and allow the enterprise to benefit from modern, cloud-native characteristics such as rapid deployment, dynamic provisioning, and resource pooling. Applications that are migrated to an infrastructure based in the cloud, connected by software-defined networks to deliver flexible, mobile, and secure access to data and analytics, will provide the resiliency and elastic capacity necessary to achieve the performance expected of large-scale applications at a reasonable cost.

Additionally, cloud migration leads to DR improvements. The current infrastructure lacks resiliency, the ability to recover quickly from failures, and does not allow for adequate DR protocols. This leaves OIT at risk of critical outages that could put CBP's mission at risk.

C.4.4 MODERNIZATION

BEMSD has a portfolio of systems and applications that range from small, serving very specific purposes for a relatively small user community, to large and complex systems, supporting a large user base. BEMSD systems and applications were built and are maintained using a diverse

technology stack and a combination of custom-developed and configured Commercial Off-the-Shelf (COTS)-based products and software. Some systems and applications are already running in a cloud environment. During the period of performance for the BEAGLE contract, modernization may include supporting BEMSD as follows:

a. Full replacement of select systems or applications, including the identification of innovative approaches and technologies, as well as the development or configuration of the modernized solution.
b. Migration of many applications to a new platform, and the migration of most applications to a cloud environment. Note that BEMSD fully understands that the migration of a system or application to a cloud environment does not constitute "modernization." Rather, CBP policy and direction require migration smartly to the cloud, and modernization may occur before or after the system or application has been migrated to the target cloud environment.
c. Application of industry- and Government-leading practices in Agile development as both an enabler to modernization and a more transparent and predictable modernization schedule.
d. Identification of innovative approaches to more effective IT portfolio delivery, management, and governance, leading to the more efficient allocation of resources, a better coordinated development and release process, and a more predictable security and Authorization to Operate (ATO) process.

C.4.5 INNOVATION

BEMSD's portfolio of systems, dependencies, and support require careful and methodical balance between performance, dependency, buying down technical debt, supporting various missions, and new functionality or systems development. In the context of this balance, BEMSD is seeking ideas that help infuse innovation into processes and approaches, system engineering, as well as in technology and, in this context, innovation should not be confused with modernization.

Innovation can also be effective as a programmatic mechanism, ensuring consistency where possible, understanding and managing resources, risks, and exceptions, and implementing the right structure and approach. Innovation by itself cannot be successful and requires the skills and knowhow to back up innovative ideas and approaches.

C.4.6 REDUCTION OF O&M SPENDING

Over the past decade the number of applications in the BEMSD portfolio has risen due to operational, mission and other statutory and regulatory requirements. Many of these applications are legacy programs that do not address future-state strategies. Additionally, many applications are duplicative in nature with a single customer focus or a gap fill-in capability. Given the nature of the CBP mission, similar technology needs are often identified by various divisions/directorates and fulfilled by their direct support offices within OIT. Furthermore, as functionality is improved or new capabilities are identified for a system in one division/directorate, these improvements are not replicated in similar systems across the enterprise, leaving mission customers with various levels of capability and ease of use in support of the CBP mission.

BEMSD is seeking an approach to reduce its IT footprint and decrease O&M spending through modernization, re-architecture, or other service oriented approaches. While no sustainment reduction cost targets have been defined, the contractor shall seek opportunities to reduce long term spending through elimination of duplicative capabilities and high sustainment cost constructs.

C.5 TASKS

Task 1: Provide TO Management

Task 2: Provide Transition-In and Transition-Out

Task 3: Provide Portfolio Management

Task 4: Provide Technology Management

Task 5: Provide Application Development and IT Security

Task 6: Provide Production O&M

Task 7: Provide Customer Services

Task 8: Provide Data Analysis, Rationalization, and Analytics

Task 9: Provide Additional Services (Optional)

C.5.1 TASK 1 – PROVIDE TO MANAGEMENT

The contractor shall provide TO management. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

C.5.1.1 SUBTASK 1.1 – COORDINATE A TO KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a TO Kick-Off Meeting at a location approved by the Government (Section F, Deliverable 03). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from each of the BEMSD mission branches, other relevant Government personnel, the BEMSD Technical Point of Contact (TPOC), and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR).

At least three business days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (Section F, Deliverable 02) for review and approval by the FEDSIM COR and the BEMSD TPOC prior to finalizing. The slide deck for the Kick-Off Meeting is a part of this Deliverable. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of contact (POCs) for all parties.
b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
c. Time Phase Labor Mix (TPLM) (with Background Investigation (BI) impact consideration) and status.

d. Updated Transition-In Plan (Section F, Deliverable 13) and discussion.
e. Draft Integrated Master Schedule (IMS) (Section F, Deliverable 11), including risks categorized as general or branch/system-specific.
f. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
g. Acquisition Risk Questionnaire (Section F, Deliverable 18; template in Section J, Attachment U)

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report (Section F, Deliverable 04) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.2 SUBTASK 1.2 – CONTRACTOR LABOR AND FINANCIAL REPORTING

The contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract. The BEMSD financial environment is complex, with funding for individual applications and systems flowing from customers through BEMSD and tracked at the application/system-level, with some base/general funding for BEMSD-wide functions such as program management and Enterprise Architecture (EA). As such, financial reporting must be granular to provide accurate forecasting.

Reports shall include:

a. Bi-monthly Cost Accrual Report: The contractor shall provide cost accruals at the sub-CLIN level (application/system), showing TO funding, fully-loaded costs accrued (including projected indirect rates and award fee), and funding balances to date. This report will assist the Government with, among other things, prioritizing remaining efforts during the period of performance, proactively communicating the need for additional funding from customers, and planning for the management of funds. These twice-monthly reports shall be delivered in alignment with the contractor's pay periods.

b. Bi-monthly Estimates at Completion (EACs): The contractor shall provide bi-monthly EAC reports that detail at the sub-CLIN level (application/system) the burn rate from the beginning of the contract period to date and the estimated remaining costs required to reach the end of the contract period from the current date. Remaining cost estimates shall be updated twice per month to reflect current trends and projected level-of-effort increases or decreases. The Government will use the reports to identify potential funding gaps (or overfunded efforts) and discuss solutions with customers. EAC reports shall be delivered twice per month on a schedule agreed upon with the Government.

Prior to the exercise of each subsequent Option Period, the contractor shall submit a TO Budgetary Rough Order of Magnitude (ROM) (Section F, Deliverable 19) to the FEDSIM COR and BEMSD TPOC no fewer than 120 calendar days prior to the end of the current contract period. For the Base Period, this ROM shall be delivered within 45 days of Project Start (Section F, Deliverable 01). This TO budgetary ROM shall detail the planned level of effort (LOE) and cost by individual application, system and/or functional area (ex. TO management, security management), with roll-up to the portfolio and overall TO-level, and shall detail to the extent

possible anticipated LOE and cost by Task for each application or system. The Government and contractor shall discuss any planned increases or decreases over the prior year's actuals in order to determine feasibility, availability of funds, and the most efficient and effective approach.

C.5.1.3 SUBTASK 1.3 – PREPARE MONTHLY STATUS REPORTS (MSR) AND CONDUCT TECHNICAL STATUS MEETINGS

The contractor shall develop and provide an MSR (Section J, Attachment F) (Section F, Deliverable 05). The MSR shall include the following:

a. Activities during the reporting period, by task (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them, as well as updates on risks and associated mitigation plans.
c. Personnel gains, losses, recruiting and hiring updates, and status (i.e., BI or security clearance, training, or certification).
d. Government actions required and dependencies.
e. Risk register, detailing project and program risks that the contractor is tracking, who the contractor's and/or Government's risk owner/tracker is, ratings on a high/medium/low basis regarding impact and probability, and proposed mitigation plan.
f. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
g. Summary of trips taken, conferences attended, and other activities (attach Trip Reports to the MSR for reporting period).
h. Accumulated invoiced cost for each CLIN up to the previous month.
i. Projected cost of each CLIN for the current month.

The contractor TO Program Manager (TOPM) shall conduct a monthly Technical Status Meeting with the BEMSD TPOC, FEDSIM COR, and other Government stakeholders (Section F, Deliverable 06). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor TOPM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned to the FEDSIM COR (Section F, Deliverable 07).

C.5.1.4 SUBTASK 1.4 – CONDUCT QUARTERLY PROGRAM MANAGEMENT REVIEWS (PMRs)

The contractor shall conduct quarterly PMRs (Section F, Deliverable 08) with the FEDSIM Contracting Officer (CO), FEDSIM COR, and other vital FEDSIM and BEMSD Government stakeholders. The PMRs shall provide both a technical/schedule review and a cost review. All PMRs shall include contractor representatives who are empowered to accept and make commitments on behalf of the contractor.

Each PMR shall address the following:

a. Financial/cost status including costs, schedule, and performance for all projects. Provide cost and financial analysis including Work Breakdown Structures (WBS), cost estimating baseline documents, lifecycle cost estimates, and cost benefit analysis for required or recommended modernization initiatives.
b. Status of all projects and updated information regarding the "health" of the high visibility projects. The "health" should include current status, risks, issues, concerns, hurdles, recommendations for improvement, and implementation strategy of recommendations.
c. Schedule status and proposed schedule changes.
d. Discussion of risks and mitigation strategies.
e. Review of contractor's issues.
f. Technical accomplishments.
g. O&M status including key events, incidents, and performance monitoring of Service Level Agreements (SLAs);
h. Review and status of deliverables.
i. Quality assurance findings and plans for corrective action.

The contractor TOPM shall provide meeting minutes (Section F, Deliverable 09), including attendance, issues and risks discussed, decisions made, and action items assigned to the FEDSIM COR within five calendar days following the meeting.

C.5.1.5 SUBTASK 1.5 – PROJECT MANAGEMENT PLAN (PMP) AND IMS

The contractor shall prepare a PMP (Section F, Deliverable 10). The contractor shall provide the Government with a draft PMP at the kick-off meeting on which the Government will make comments. The final PMP shall incorporate the Government's comments.

The PMP shall, at a minimum:

a. Describe the proposed management approach.
b. Describe in detail the contractor's approach to risk management under this TO, to include supply-chain risk management (SCRM).
c. Describe in detail the contractor's approach to enterprise communications, including processes, procedures, communication approach, and other rules of engagement between the contractor, BEMSD branches, other BEMSD contractors providing application development and security, and FEDSIM.
d. Contain a decision log to provide a concise, centralized record of all decisions, approvals, or agreements affecting the scope, schedule, or internal and/or external deliverables for the TO.
e. Contain a Communication Plan to identify and track all required communications in support of the PMP, which identifies all key stakeholders and appropriate communications format (such as meetings, briefings, SharePoint), content, and schedule for each stakeholder.
f. Contain a tailored Quality Management Plan that identifies the contractor's approach for providing and ensuring quality in meeting the requirements of this TO, including identifying the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives.

g. Detail Service Level Agreements (SLAs) under the TO (Section F, Deliverable 17). Draft SLAs shall be drafted as a part of the draft PMP due at the Kick-off Meeting. Final SLAs shall be delivered as a part of the Final PMP. The contractor may choose to propose updated or suggested SLAs each award fee period, no fewer than 30 calendar days prior to the start of the subsequent award fee period, with approved SLAs being incorporated into the TO.

The PMP is an evolutionary document that shall be updated annually at a minimum.

The contractor shall maintain a resource-loaded IMS (Section F, Deliverable 11) that allows the contractor to accurately manage schedules and resources across the TO, identifies tasks or applications that are over- or under-resourced so that staffing reallocations or efficiencies can be quickly identified and realized, and provides the Government with an understanding of milestones and Government dependencies. A draft IMS is due at project kick-off. The Government will provide comments, and the final IMS template shall incorporate the Government's comments.

The IMS shall, at a minimum:

a. Provide for an overall WBS with a minimum of three levels and associated responsibilities and partnerships between Government organizations;
b. Include milestones, tasks, and subtasks required in this TO.
c. Identify the schedule and personnel resources for all work efforts under this TO, ensuring that schedules are appropriately resource-loaded and that individual resources are not over-utilized;
d. Clearly identify Government dependencies that affect the critical path of project schedules, and identify the communication method used to ensure the appropriate Government stakeholders are notified of such dependencies in a timely manner.
e. Be delivered in a commonly-available COTS software file format that allows the clear identification of milestones and assignment of resources (such as Microsoft (MS) Project or some other format that the contractor deems appropriate).

The contractor shall brief updates to the IMS on a monthly basis to the FEDSIM COR and BEMSD Government leads, focusing on critical Government dependencies, schedule risks, and upcoming 30/60/90-day schedules. The updated IMS shall be incorporated into the PMP. The contractor shall work from the latest Government-approved versions of the PMP and IMS.

C.5.1.6 SUBTASK 1.6 – INTEGRATED OPERATIONAL DASHBOARD

The contractor shall create and maintain an Integrated Operational Dashboard ("the dashboard"). The contractor's proposed dashboard shall use existing software tool(s) already integrated into the BEMSD architecture; no new software tool shall be introduced. At a minimum, the dashboard shall report:

a. Real-time status of active projects.
b. Daily service desk ticket queues.
c. Status of BEAGLE contractor personnel awaiting CBP BI adjudication, showing present status (paperwork submitted, delayed, partial/initial, or other status as appropriate), and highlighting those experiencing significant delays.
d. Real-time operational status of applications under BEAGLE management.

The dashboard shall be a quick reference for TO and Government management to determine the health of the enterprise. The initial version of the dashboard shall be presented to the Government as soon as possible after the completion of transition-in, but No Later Than (NLT) six months after TO award.

C.5.1.7 SUBTASK 1.7 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (Section F, Deliverable 12). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. The contractor shall utilize the applicable BEMSD IT application (Overtime and Travel (OT&T)) for trip requests. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained or information collected. At a minimum, trip reports shall be prepared with the information provided in Section J, Attachment G.

C.5.2 TASK 2 – PROVIDE TRANSITION-IN AND TRANSITION-OUT

Transition-in ensures the smooth and orderly transition from the current contract. Transition-out ensures all knowledge, data, material, and information developed by or provided to the contractor is transitioned and delivered to the Government by the end of the TO.

C.5.2.1 SUBTASK 2.1 – TRANSITION-IN

The contractor shall ensure a smooth and orderly six-month transition-in period. Transition shall begin immediately upon TOA, and staffing shall be phased in over time as the existing BEMSD IT contract expires.

Transition-in shall be completed after the following:

a. All tasks are fully staffed with fully-qualified and trained personnel in accordance with (IAW) the Government-approved Transition-in Plan's TPLM.
b. The contractor assumes full responsibility for management of all TO requirements.
c. All TO performance measures are in force and enforced.
d. No further support is required from the outgoing contractors.
e. The Transition-In Plan has been fully executed.

The contractor shall update the draft Transition-In Plan and TPLM on or before project kick-off for Government approval (Section F, Deliverable 13). The contractor shall submit its Final Transition-In Plan and TPLM within ten workdays of receipt of Government comments on the draft Transition-In Plan and TPLM. The Transition-In Plan shall culminate with final transition achieved NLT six months after award and include measurable milestones and decision gates (with entrance and exit criteria) for Government review. The TPLM shall identify all personnel and positions to transition to the TO, when they transfer, and their role. The Government will review and accept this TPLM as the initial baseline.

C.5.2.2 SUBTASK 2.2 – TRANSITION-OUT

The contractor shall develop a draft Transition-Out Plan (Section F, Deliverable 14) for facilitating the accomplishment of a seamless transition and delivering all material and information from this TO to an incoming contractor and/or Government personnel at the expiration of the TO. The draft Transition-Out Plan shall identify all Government-Furnished Property and Contractor-Furnished Property (GFP/CFP) as well as information and material developed during the TO that was used in the execution of this TO. The draft Transition-Out Plan shall be submitted for Government approval. Upon incorporation of comments and Government acceptance, the contractor shall follow the Final Transition-Out Plan to transfer all material, information, and rights thereto to the Government.

The contractor shall provide a Transition-Out Plan NLT 180 calendar days prior to expiration of the TO.

The contractor shall facilitate and conduct transition-out activities. The contractor shall update system descriptions and technical descriptions of all software, systems, and mission-support activities delivered or performed under this TO. The contractor shall support transition of administrative and privileged access to the incoming contractor, ensuring that no administrative access is lost. The contractor shall prepare a final report documenting the status of all ongoing efforts and projects and a smart book/turnover binder containing copies of all plans, policies, procedures, POCs, file storage locations for technical diagrams and documentation, institutional knowledge, and other information requested by the Government. Transition-out shall ensure no disruption to vital Government business. The contractor shall provide full cooperation in providing necessary operational knowledge to the incoming contractor.

Transition-out shall include the following types of services:

a. Project management processes.
b. Identification of POCs.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives and projects.
e. Incumbent contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel.
g. Identification of schedules and milestones.
h. Identification of actions required of the Government.
i. Establishment and maintenance of effective communication with the incoming contractor and Government personnel for the period of the transition via weekly status meetings.

C.5.3 TASK 3 – PROVIDE PORTFOLIO MANAGEMENT

The contractor shall provide Portfolio Management including IT governance, portfolio prioritization, planning and budgeting functions including the development of application business cases, burn reports, administrative assistance, and ad-hoc reports within the BEMSD portfolio.

C.5.3.1 SUBTASK 3.1 – PROVIDE BEMSD IT GOVERNANCE

BEMSD is seeking to strengthen its IT Governance framework and provide standardization in areas such as SecDevOps, requirements/stories capture management, technical documentation, policy management, change control process phases, configuration, security, SCRM, assessing and authorizing IT management, planning and implementation control, post-implementation review, closure, and formalized measurement, testing, as well as auditing- and compliance-readiness.

The contractor shall facilitate BEMSD governance boards (e.g., Architecture Review Boards (ARBs), Change Configuration Boards, Change Management, Cyber Security meetings, and other technical meetings and boards as directed), including the review of projects entering the execution pipeline, reviewing the forecast of upcoming releases, and leading discussions regarding schedule, conflict, and resolutions.

The contractor shall mature the BEMSD IT posture and capabilities while adhering to the policies and processes established by the Government's process improvement initiatives and in accordance with industry best practices such as Carnegie-Mellon's Capabilities Maturity Model Integration (CMMI) and Information Technology Infrastructure Library (ITIL).

C.5.3.2 SUBTASK 3.2 – PROVIDE PLANNING, BUDGETING, AND APPLICATION BUSINESS CASES

The contractor shall provide overall portfolio management assistance, including planning, scheduling (including resources, duration times, dependencies, and start and end dates), tracking, project cost estimations, and overall financial management/budgeting for BEMSD portfolios and projects across the application lifecycle. The contractor shall assess the BEMSD application portfolio for opportunities to optimize the mission and develop business cases for application disposition. The contractor shall be proactive in recommending BEMSD IT solutions as issues arise and play an active role in their resolution.

Additionally, as part of portfolio planning, the contractor shall investigate and evaluate opportunities for new technologies including:

a. Efforts to retire legacy applications (migrating into modernized constructs).
b. Efforts to improve business processes.
c. Efforts to improved system/facility operations.
d. Efforts to address compatibility or interoperability issues within existing systems and effect on operating environments.
e. Other efforts as directed by the Government.

The contractor shall maintain knowledge of, and adhere to, applicable laws, regulations, and security and audit/compliance requirements governing IT programs within the BEMSD portfolio, and bring to the attention of the appropriate BEMSD manager the impact of new or changing laws, regulations, and security requirements.

C.5.3.3 SUBTASK 3.3 – PROVIDE BEMSD CONTINUOUS IMPROVEMENT PROGRAM

The contractor shall establish a Continuous Process Improvement (CPI) program with the objective of reducing costs while improving quality and mission effectiveness. Cost reductions

and innovations that are accompanied with demonstrated quality improvements will be rewarded in accordance with a scheme proposed by the contractor (e.g., earned award fee) and approved by the Government in the Performance Requirements Summary (PRS) and award-fee activities.

The contractor shall identify and propose discrete innovation projects for Government approval (Section F, Deliverable 15). These innovation projects are not limited to each project portfolio within BEMSD, but may also be across portfolios and CBP wide. Each innovation project shall include the following information as a minimum:

a. Estimated cost savings or cost avoidance.
b. Expected and measurable improvements to quality or mission effectiveness.
c. Timeline for implementation.
d. Government provided material, information, assistance, and funding.

For each Government-approved innovation project, the contractor shall prepare and submit an Innovation project implementation plan within 30 calendar days (Section F, Deliverable 16). The Government will prioritize these projects and authorize a start date for each. The contractor shall manage innovation projects the same way as all other work, including tracking and reporting estimated and actual/realized cost savings or cost avoidance as well as realized quality and mission effectiveness changes (positive or negative) for each Government-approved innovation project.

C.5.4 TASK 4 – PROVIDE TECHNOLOGY MANAGEMENT

The contractor shall provide application migration planning strategies, engineering and architecture services, analysis of embedded technologies and recommendations for modernization opportunities, integration approaches and standardization recommendations, and IT asset management.

C.5.4.1 SUBTASK 4.1 – PROVIDE APPLICATION MIGRATION PLANNING

BEMSD has identified more than 60 applications, plus supporting databases, that currently reside in unclassified data centers. BEMSD intends to migrate most of these applications from these data centers over the course of this TO (excepting those where cloud hosting is not technically possible). The lease for the current CBP-run data center expires in 2024. Applications may be migrated to commercial cloud providers, application-specific providers, or other service providers based on the results of application planning. During migration, migration plans should account for additional resources to deliver task activities, including, but not limited to, customer services that may need to increase in order to effectively support users and applications that are currently provided by legacy hosted centers. The contractor shall coordinate with the Government to schedule and perform migration, while maintaining high levels of availability for applications.

The contractor shall analyze the current BEMSD IT cloud migration strategy and provide an application migration plan (Section F, Deliverable 20). The plan shall identify opportunities to gain efficiencies in the following areas:

1. Reduce migration timeline.

2. Improve quality of application migration plans.
3. Reduce/eliminate duplicate data across branches (databases).
4. Establish technology refresh requirements/needs such as updating code to latest versions.

The contractor shall maintain the application migration plan from planning through application migration, and shall incorporate lessons learned for future migrations and across the BEMSD portfolio under BEAGLE.

C.5.4.2 SUBTASK 4.2 – PROVIDE ENGINEERING SERVICES

The contractor shall develop the engineering design to provide the business and operational requirements for either new systems, enhancements to existing systems, or replatforming existing systems; interacting with the project teams and individual applications.

The contractor shall define and ensure standard engineering designs, templates, processes, and procedures for implementing projects that follow approved BEMSD IT architectures.

The contractor shall update or develop, where appropriate, baseline system documentation that includes system designs, build procedures, requirements documents, test procedures, PRs, software code, and system knowledge base and deliver to the Government upon final Government acceptance of the baseline (Section F, Deliverables 21, 22, and 23).

The contractor shall provide continuous leadership, innovation, monitoring, control, and management of engineering changes and provide a forum to facilitate and encourage collaboration between key stakeholders.

C.5.4.3 SUBTASK 4.3 – ARCHITECTURE AND INTEGRATION SERVICES

The contractor shall prepare detailed technology roadmaps and transition planning of applications (Section F, Deliverable 24). The contractor shall support BEMSD in prioritizing the integration and scaling of BEMSD-preferred technologies and systems include promoting wider CBP acceptance and use. This includes both hardware and software-based solutions.

The contractor shall provide detailed technology integration assessments and impact analyses (Section F, Deliverable 25). The contractor shall conduct analyses and identify technologies to enhance the BEMSD suite of applications, capitalizing on advancements in software development, automated testing approaches, release methodologies, interface and integration technologies, interface and integration management, software security, mobile computing, data modeling, management and storage, and hosting environment. Each analysis should consider contractor availability, maintainability, expandability, reliability, security, and financial implications.

The contractor shall develop/maintain architectures to ensure that standardized best practices are utilized, integral to all operations involving any application to be deployed. The contractor shall seek to implement service oriented concepts. Architecture documentation will include products in the analysis, design, detailed design, and build phases, such as, but not limited to:

a. Generalized and detailed schematics.
b. Design and solution strategies.
c. High-level and detailed process flows.

d. Information assurance (IA).

e. Disaster recovery and business continuity capabilities.

f. Configuration specifications.

g. Testing specifications.

The contractor shall focus on optimizing productivity and product quality, while reducing the occurrence of inefficient systems and processes, through standardized architectures. The contractor shall also focus on ensuring technological and process approach consistency across programs and shall maintain guidelines for technical direction, and demonstrate adherence to these guidelines, tracking approved options for use. Design concepts shall include provisions for technology refreshes that will capitalize upon emerging technological advances available in COTS product offerings. The contractor shall inform and advise the Government on cross-cutting architecture and technical issues that may impact the enterprise.

C.5.4.4 SUBTASK 4.4 - PROVIDE DR/CONTINUITY OF OPERATIONS (COOP) FOR BEMSD APPLICATIONS

The contractor shall perform analysis of the BEMSD applications in order to establish, maintain, update, and/or develop plans, processes, procedures, and training materials for restoration of operations in the event of an incident or disaster. In accordance with existing BEMSD IT DR and COOP policies and procedures (see DHS 4300A, "Sensitive Systems Handbook"), the contractor shall review and provide input to plans as required, including as a part of the renewal of application ATOs or system controls review during Ongoing Authorization (OA), further defined in C.5.5.3.

The contractor shall support BEMSD and CBP COOP exercises, such as planned virtual events and table top exercises. The contractor shall ensure that applications are designed in a resilient manner and take into account disaster recovery and failover capabilities as a part of their design. Applications designated as "Mission Critical" in the BEMSD Incident Classification and Response Guide under the BEMSD IT portfolio require a 72-hour failover timeline restoration.

C.5.4.5 SUBTASK 4.5 – PROVIDE IT ASSET MANAGEMENT

The contractor shall track and maintain assets (hardware and software data) using SAP, the BEMSD SharePoint database, or other Government-approved asset management tracking system for all IT applications within the BEMSD IT portfolio to include full visibility of and accountability for all Government furnished equipment and tools, deployed hardware, software, IT assets, and COTS software license and warranty management information, for assets acquired by the Government for this TO.

C.5.5 TASK 5 – PROVIDE APPLICATION DEVELOPMENT AND IT SECURITY AND ACCREDITATION

The contractor shall perform all activities necessary to institutionalize and adhere to a standardized SecDevOps path to production that accounts for speed, scalability, predictability, and quality, as well as for any coaching required to achieve this objective. This objective applies to all BEMSD development activities, including requirements, design, application development

and retiring technical debt, testing and release, deployment, O&M, and migration of BEMSD applications and systems. BEMSD is seeking to instantiate a SecDevOps methodology to software development and O&M based on industry- and Government-best practices. The contractor shall support a transition to SecDevOps where one does not currently exist for a given system or application, and a path to production through implementation of automated testing and validation capabilities in collaboration with software developers, while maintaining a secure application posture. The contractor shall leverage SecDevOps implementation methods, such as feature demonstrations and cycle planning events to provide much more frequent and valuable information, on which BEMSD and product owners can engage to make sure the best value is being created.

C.5.5.1 SUBTASK 5.1 – PROVIDE SOFTWARE DEVELOPMENT APPROACH

The contractor shall use industry- and Government-best practices for secure software design and development methodologies to ensure that applications placed into a production environment conform to CBP OIT system security requirements and do not have security vulnerabilities.

The contractor shall provide a Software Development Plan (SDP) (Section F, Deliverable 27) and approach that leverages the structure and speed that Agile services can provide, but adheres to requirements for documentation and compliance from CBP, and from DHS via CBP-adopted or tailored requirements. The contractor shall update the SDP on a periodic basis as CBP or DHS policy changes or improved methodologies or procedures are developed, but no less than annually. Refer to Section H.6 for a listing of applicable DHS and CBP IT governance documents and frameworks.

The contractor shall continuously assess and optimize the performance of processes within the BEMSD IT enterprise, including the path and process by which capabilities and applications are introduced into the production environment. The contractor shall recommend areas of innovation that help optimize and automate the IT capability path-to-production to accelerate response time to customer service requests and deliver new capabilities.

C.5.5.2 SUBTASK 5.2 – PROVIDE APPLICATION DEVELOPMENT

The contractor shall provide qualified technical and management personnel resources to accomplish the implementation of capabilities that bridge traditional or iterative approaches with Agile-specific capabilities. The contractor shall develop new applications IAW cloud-ready and/or mobile architectures to support smart cloud migration and/or mobile capabilities.

The contractor shall utilize efficient and effective best practices across all application development phases, e.g. planning, design, development, testing, and deployment to manage agile teams, ensuring high levels of velocity are maintained and can be readily qualified. For sprints, BEMSD currently utilizes JIRA and Team Foundation Server (TFS), depending on the branch or application. In the BEMSD portfolio, applications have sprint cycles of two to three weeks.

The contractor shall provide requirements management, including defining, documenting, sequencing, and traceability of functional, technical, and security-related requirements. The contractor shall update documentation such as Context Diagrams, Use Case Models, User Stories, and associated design documentation for new requirements and iterations of an

application or system (Section F, Deliverable 28). The contractor shall assess and document the impact of new functional requirements on the existing design baseline.

The contractor shall provide expertise to capture, analyze, manage, and verify requirements as well as perform integration analysis in order to ensure application development projects are compliant and seamless to the user. The contractor shall develop a WBS for BEMSD IT applications, identifying critical tasks and timelines to successfully sustain applications.

The contractor shall provide application development planning to include:

a. Coordinating and facilitating customer and stakeholder sessions.
b. Performing gap analysis activities.
c. Providing Analysis of Alternatives (AoA), in order to assist BEMSD to develop ROM determinations (Section F, Deliverable 30).
d. Developing test plans and planning integration activities.
e. Developing and maintaining security paperwork.
f. Developing a WBS identifying key activities and critical paths for successful development efforts.
g. Performing project configuration and technical compliance review planning requirements.
h. Providing technical expertise to assist Technical Lead/TOPM in various CBP and DHS Exit Gate reviews, as required.
i. Developing and maintaining a Requirements Traceability Matrix (RTM) and proactively managing risk for all requirements that are part of application development.
j. Analyzing user stories for size and requirements and provide methodologies to explain their estimations and strategies, including for the reduction of product backlog.

The contractor shall perform application design activities to include:

a. Developing DHS and CBP Lifecycle tailoring document(s).
b. Specifying software design changes for applications based on user requirements (analysis).
c. Providing all associated DHS/CBP Systems Lifecycle (SLC)-compliant documentation, as required.
d. Providing all associated CBP Architecture Alignment and Assessment (AAA)-compliant documentation as directed by the Government or, when not explicitly specified, as appropriate to demonstrate adherence.
e. Providing all associated DHS Alignments (Milestone Decision Points)-compliant documentation as directed by Government or, when not explicitly specified, as appropriate to demonstrate adherence.
f. Maintaining application design documentation using the Government furnished document management system or, when not explicitly specified, as appropriate to define the application.
g. Employing design patterns that ensure code simplicity, address users' needs, and enable future maintainability.

h. Providing designs which are adaptive to volatile, evolving, and urgent system and/or operational requirements.
i. Utilizing Infrastructure as Code (IAC) as a practice, where applicable, enabling the cloud's Application Programming Interface (API)-driven model to interact with infrastructure programmatically.

The contractor shall perform application development which provides for rapid delivery in small batches with high frequency and pace of releases, and the application of continuous integration and continuous delivery practices. The contractor shall provide full documentation of any application changes and/or modifications to the existing systems software, as specified by the Government or, when not explicitly specified, as appropriate to define changes. The contractor shall also provide:

a. Technical methods, techniques, and concepts that are innovative, practical, cost-effective, and conducive to CBP's processes and development standards.
b. Applications developed based on requirements that are evolving and emerge as the mission needs or business requirements shift.
c. Monitoring, system alerts, and logging practices to help stakeholders stay informed of performance in real-time, and be able to proactively address potential problems.
d. Collaboration and cooperation with Government and other contractor teams to improve the user experience, to baseline and re-establish key performance parameters for the system, and to address all gaps as part of continuous improvement and collaboration.
e. Fixes for escaped defects within a time frame consistent with SLAs for the given application or system.

The contractor shall maintain high code quality, as documented in its software development and quality management processes. The contractor shall:

a. Develop high quality secure code and shall be responsible for any technical debt (design debt or code debt) that is incurred as a result of their development activities.
b. Incorporate monitoring solutions (for example, Hygieia or New Relic) or recommend other approaches. The contractor may suggest new methods or tools; however, developers shall add health checks to code so that monitoring tools can detect changes with appropriate metrics.
c. Ensure that the system has built-in quality, by prioritizing Availability, Maintainability, Vulnerability, and Reliability.
d. Work to increase the code coverage and code quality, as per industry best practice and/or as directed by the Government.
e. Proactively assist the Government in eliminating existing technical debt and rewriting issues to remove bad designs and security issues from the code base and provide clear, value-based support of these decisions.
f. Ensure code meets the functional and Non-functional Requirements (NFR), such as performance, security, and capabilities; meets database development requirements; meets testing requirements; and is deployable and fully tested.

The contractor shall provide testing, integration, and deployment release services. BEMSD is seeking to automate testing as part of SecDevOps. Testing often requires frequent engagement with the end-user community, stakeholders, and designated representative testers. Development and testing shall include use of automated regression test techniques as part of a continuous software integration process. The contractor shall ensure all products are thoroughly tested, including stress and boundary testing. Throughout the software development process, the contractor shall identify and correct product test issues.

The contractor shall develop and deliver test procedures, test data, materials, results, and artifacts (Section F, Deliverables 21, 22, and 23). The contractor shall conduct appropriate tests consistent with the developmental methodology (e.g., unit, functional, system, interoperability, regression, security, and performance) of software throughout the development lifecycle using industry best practices of continuous integration methods and automated regression test utilities. Test materials (e.g., scripts, configurations, utilities, tools, plans, and results) shall be maintained under configuration control. The contractor shall provide all testing services as necessary to correct test problem reports prior to production implementation. Specifically, the contractor shall:

a. Migrate system components in accordance with CBP OIT requirements, from development to testing, and subsequently, to the production environment.
b. Perform testing and configuration control in preparing for production implementation.
c. Create test cases, automate test scripts for test automation activities, and thoroughly test the code (Section F, Deliverable 23).
d. Collaborate with other teams to support test-driven and continuous code integration.
e. Provide testing and Software Quality Assurance (SQA) as necessary to correct test problem reports.
f. Share test scripts (manual and automated), as needed and with BEMSD approval, with other testing entities.
g. Thoroughly test changes and remediate all known security issues before committing them into the CI/CD pipeline and document all testing scenarios applied against the change.
h. Perform alpha and beta testing. The contractor shall assist with constructing validation steps (both positive and negative testing) for user acceptance testing on an as needed basis.
i. Perform integration and configuration within and across teams to ensure the automatic build and deployment process works effectively across all environments, including the contractor's development/test enclave. Deployment and testing in the development/test environment should mimic closely the actions performed for deployment and testing in staging and production. The contractor shall leverage the OpenShift Platform (or identified equivalent) to the fullest extent possible.
j. Perform deployment release functions, ensuring that all scheduled outages needed for will be approved by the Government. The contractor shall use standardized methods and procedures for efficient and prompt handling of all changes in order to minimize the impact of change-related incidents upon service quality.
k. Ensure clear communication and coordination with users throughout the development, testing and release processes, and coordinate any necessary training (see C.5.7 – Customer Service).

C.5.5.3 SUBTASK 5.3 – PROVIDE IT SECURITY AND ACCREDITATION

The contractor shall provide cyber security compliance, IA oversight and management, Certification and Accreditation (C&A), and the required security services for current and future systems maintained under this contract, including certified Information Systems Security Officers (ISSOs). These services shall be delivered using a systematic, disciplined approach to evaluate risk management, information security controls, COOP/DR capabilities, and governing processes. Currently, BEMSD manages approximately 30 ATO packages.

The contractor shall apply the Risk Management Framework (RMF) throughout the system lifecycle to identify, implement, assess, and monitor all applicable security controls. The contractor shall author and develop all RMF artifacts required in support of accreditation including the Security Plan (SP), Security Assessment Report (SAR), Security Controls Traceability Matrix (SCTM), and Plan of Action and Milestones (POA&M).

Security accreditation is part of a dynamic, ongoing risk management process. DHS is implementing OA, which involves shifting from periodic to ongoing assessments and facilitates a continual state of awareness. DHS is implementing OA in three layers, which collectively ensure constant control assurance:

- Layer 1: Common and Inherited Controls and Reciprocity
- Layer 2: Continuous Monitoring
- Layer 3: Event-Driven Monitoring

The contractor shall provide continuous monitoring to supplement and reinforce the security accreditation to allow for OA. The contractor shall use continuous monitoring to:

a. Track any changes to systems or applications.
b. Analyze the security impact of those changes.
c. Make appropriate recommendations, and once approved make adjustments to the security controls and the system security plan.
d. Report the security status of the system IAW CBP OIT and BEMSD guidelines and processes for system and cyber security.

The contractor shall follow 12 Factor App development practices (12factor.net), cloud native (cncf.io), NIST RMF, building/deploying microservices within CBP's Continuous Integration, Continuous Delivery (CI/CD) pipeline, and deploying software with zero downtime. The contractor shall stay current with industry best practices as they evolve.

The contractor shall ensure that agile teams implement proactive approaches to reduce vulnerabilities and to improve responsiveness to unforeseen events, ensuring that the application development is compliant with the CBP's security policies in order to safeguard the system against external and insider threats. The contractor shall utilize SecDevOps processes to ensure compliance with and readiness for all ATO requirements and perform deployments of some or all code in accordance with CBP policy and as directed by the Government.:

The contractor shall provide security-related guidance to BEMSD and serve as liaison to OIT, CBP, and DHS security groups on security-related matters, as well as annual assessments of BEMSD production applications required to maintain C&A.

The contractor shall perform coordination of security-related audits and reviews and maintain required security documents to obtain and retain systems C&A.

The contractor shall design, develop, build, remediate, and test systems to meet security controls and ensure systems are configured in accordance with applicable standards and other compliance directives.

Security controls shall be implemented consistent with CBP architectures and policies, employing standard system engineering methodologies and security engineering principles. The contractor shall follow CBP policies as well as NIST 800-53 standards to prevent and identify vulnerabilities and implement corrective actions.

Additionally, the contractor shall implement and adhere to DHS and CBP guidelines with regards to the following processes:

a. Asset management.
b. Vulnerability management.
c. Configuration management.
d. Log integration.
e. Security Information Event Management (SIEM) integration.
f. Near real-time security status information to BEMSD personnel.

C.5.5.4 SUBTASK 5.4 – PROVIDE SYSTEM ASSESSMENT, COMPLIANCE, AND EVALUATION READINESS SERVICES

CBP OIT and BEMSD are audited each year by stakeholders both internal (ex. Office of Inspector General (OIG)) and external Independent Public Accountants (IPAs) (ex. annual KPMG audit). The Government typically requires assistance in collecting information and answering questions in regards to many broad IT areas including, but not limited to: security management controls, access controls, provisioning and deprovisioning, transfers, separation of duties, configuration management, contingency planning, application security, business process controls, interface controls, and data management system controls.

Audits of BEMSD and CBP OIT systems are wide-ranging and require the contractor to provide in-depth knowledge and expertise of many different federal standards and policies in order to support BEMSD with identifying the appropriate data and artifacts and assisting in response formulation. Such standards and policies include, but are not limited to:

- Government Accountability Office (GAO) auditing practices;
- Responding to Congressional requests for information;
- Federal Information Security Management Act (FISMA) standards and auditing practices including Federal Information Systems Control Audit Manual (FISCAM)
- Office of Management and Budget (OMB) Circular A-123;
- DHS 4300A and CBP 1400-05D security policies and manuals; and
- National Institute of Standards and Technology (NIST)
- Payment Card Industry Data Security Standard (PCI DSS)

The contractor shall provide internal assessment, compliance, and evaluation readiness services to the BEMSD organization, as well as with other CBP OIT directorates as deemed necessary by BEMSD leadership. These services include, but are not limited to:

- Provide subject matter expertise to BEMSD leadership during executive-level briefings and meetings, both on a recurring and ad-hoc basis;
- Verify and confirm that IT financial and access controls are in place and effective (especially with considerations in these areas as applications are migrated to cloud hosting services); and
- Provide strategic advice and guidance to the BEMSD Security and TIO teams regarding IT security controls best practices and implementation strategies for new systems and applications that come into the BEMSD or (as directed) CBP OIT portfolios (ex. implementing boundary controls).

The contractor shall provide liaison services between auditors and the BEMSD organization, as well as with other CBP OIT directorates as deemed necessary by BEMSD leadership. The contractor shall participate in external oversight audits as needed, coordinate, document, and review inquiries and responses with the appropriate BEMSD Government personnel, and finalize the scope of the responses to align with the requested information. Liaison services include, but are not limited to:

- Coordinating meetings between auditors, third-party Government intermediaries (such as the OIT Audit Liaison), and the appropriate BEMSD personnel; and
- Supplying auditor-requested documents or system extracts in a timely manner to the appropriate BEMSD or (upon BEMSD direction) the appropriate CBP audit liaison. Typical requests include, but are not limited to: log samples, standard operating procedures, proof of successful backup and recovery, current asset inventory, security documentation for specific users, security configuration/settings for specific infrastructure or business system components, security profiles across a given component, and user access controls and rights.
- For planning purposes approximately 8-12 compliance-related readiness reviews/audits take place each fiscal year.

The contractor shall maintain an Audit Readiness Assessment and Report, with updates provided on a weekly basis. The report shall provide a holistic view of the security and audit-readiness posture of all applications under BEMSD management, and details things such as (but not limited to) the assigned ISSO by system, nature of the system, ATO type and expiration date, latest date that various scans were run, POA&M count and status, and more. The initial template of this report is provided as an attachment to the BEAGLE TO (Section J, Attachment I). As new applications and systems come into the BEMSD portfolio, the contractor shall incorporate them into the report.

The contractor shall provide a weekly audit status tracker to BEMSD leadership that details, at a minimum, the status of all audit responses under BEMSD management and the proposed resolution date for those actions. Beyond this work product, the contractor shall actively

participate in and provide proactive communications to the Government regarding new and emerging actions and issues.

C.5.5.5 SUBTASK 5.5 – PROVIDE CERTIFIED RECORDS REQUEST AND FREEDOM OF INFORMATION ACT RESPONSE SUPPORT SERVICES

BEMSD receives Certified Records Requests (CRRs) from the CBP Privacy & Diversity Office (PDO) and the CBP Office of Chief Counsel (OCC) on both the SEACATS and e3 applications. As of March 2020, the historical level of effort for responding to CRRs on SEACATS has been roughly 0.5 FTEs, and lower for e3 (fewer than 10 CRRs per year); however, this could increase or decrease going forward. Additionally, BEMSD also receives Freedom of Information Act (FOIA) requests on SEACATS that must be responded to; these have historically not been of a high volume.

The contractor shall provide support services for CRRs as outlined in the BEMSD Certified Records Request Process document (version 1.0 or latest), found on the CBP BEMSD Confluence page. These services include responding to Government requests for information where analysis of the BEMSD systems and data is required as input to Government responses to internal Government and third-party inquiries, in accordance with the CRR Process document. With regards to SEACATS FOIA requests, the intake and response procedures generally follow the same steps as the aforementioned CRRs, but can have more variability in the search parameters due to the nature of the information requested.

C.5.6 TASK 6 – PROVIDE PRODUCTION OPERATIONS AND MAINTENANCE (O&M)

O&M is the configuration or customization of COTS software and/or coding of custom software to correct, performance-tune, and/or make minor modifications to existing systems for initial or emerging functional requirements in order to keep systems operating, secure, and performing optimally. Maintenance may require some new development as a consequence of changes in business processes, other applications, or the retirement of buy-down of technical debt, but any new development shall continue to fulfill the requirements of the system as originally defined. O&M activities shall also cover the responsibility for existing systems in the production environment (e.g., review of system sizing based on current usage, update of code/tables in response to organization/business process changes, incident management in the event of application/environment degradation or outage). Maintenance shall include both preventive maintenance activities (e.g. applying patches and upgrades before system failures) and corrective maintenance activities that remediate system failures or defects after they have been identified.

The BEMSD IT portfolio is comprised of multiple legacy and modernized applications of varying architectures. The contractor shall provide IT O&M services that are established through problem tickets, statutory and regulatory directives, CBP OIT policies, as well as various security patches. Security compliance and patch management is a crucial element of IT O&M. IT security planning, implementation, and compliance is integral to all work performed at BEMSD and, therefore, coordination with stakeholders is critical to ensure that patches to vulnerabilities

are quickly remediated. The contractor shall comply with DHS Continuous Diagnostics and Mitigation (CDM) program requirements. The contractor shall provide awareness and coordination of patching and malware management with appropriate organizations within OIT.

The contractor shall sustain system baselines and software applications, ensuring timely security and product updates and quality releases. The contractor shall provide O&M to sustain the hardware and software capabilities of the lab in Williston, Vermont (VT), including the sustainment of production, the timely update of security, incorporation of new functionality and/or new sensor device types, and adherence to high quality and responsiveness to the clients' needs. The contractor shall support the Government in developing requirements, test, and integration plans and resolving issues in accordance with the criticality of the systems, including responsibility for both existing systems and the deployment(s) of new releases and technologies.

C.5.6.1 SUBTASK 6.1 – PROVIDE O&M FOR BEMSD APPLICATIONS

The contractor shall provide all O&M activities for BEMSD applications and systems including optimizing the release of maintenance activities and providing timely scheduled maintenance.

The contractor shall develop a Configuration Management Plan (CMP) (Section F, Deliverable 29) and establish and maintain a strict change control process. The change control process shall include Applications, Data Stores, and Documentation. The contractor shall follow standardized CCB processes governed by DHS Policy 4300A ("Sensitive Systems Handbook") and CBP Security Policy 1400-05D as well as standard National Institute of Standards and Technology (NIST) directives, ensuring that all changes to the system go through development and testing before they are moved into production.

The contractor shall ensure the configuration management of requirements such as software and Engineering Change Proposals (ECPs) in response to security vulnerabilities, directed architecture changes, policy/regulatory changes, legislative changes, interface changes, Business Process Improvements (BPIs), and environmental changes. The contractor shall manage strict version control on all software source code and related artifacts either acquired or developed. The contractor shall maintain the baselines and documentation for all system releases, and monitor and report the installation status of each new release. The contractor shall utilize standardized tools to provide configuration management, applying disciplined configuration management throughout the entire lifecycle of technologies.

The contractor shall utilize standardized methods and procedures for efficient and prompt handling of all changes to minimize the impact of change-related incidents and improve day-to-day operations of applications. The contractor shall consider a holistic view of a change to an IT service and ensure that all aspects of a release, both technical and non-technical, are considered together, thereby reducing potential production outages.

The contractor shall provide system sustainment services for software applications, database applications, and other solutions, including all the associated activities required to enhance, integrate, implement, and maintain the BEMSD portfolio.

The contractor shall provide expertise to capture, analyze, manage, and verify requirements as well as perform integration analysis in order to ensure IT O&M are compliant and seamless to the user.

The contractor shall conduct activities including system software maintenance and updates including security patches, hot fixes, application updates, and upgrades, and it shall ensure compliance with IT security requirements, user account management, configuration management, system upgrade/improvement, computing operations, maintenance of systems documentation and procedures, and contingency planning.

The contractor shall coordinate maintenance and repairs with vendors per published schedules or when necessary, due to hardware or software failures. The contractor shall coordinate patches or changes that require system or application downtime with the Government and schedule during allotted maintenance hours.

Additionally, the contractor shall:

a. Be responsible for the operation in production of the capabilities it develops.

b. Provide Root Cause Analysis (RCA) on all outages with actionable recommendations on how to prevent issues going forward.

c. Develop application health monitoring and alerting functions into the system, ensuring the system is monitored effectively, and reveal any production issues when they happen.

d. Provide monitoring to reveal user analytics and interactions, and provide the capability to automatically report on such activities.

e. Develop automated capabilities to monitor dependency and network-related production issues, providing the capability to rule out application issues.

f. Provide services including, but not be limited to, problem analysis, systems analysis, program modifications, changing help screens, rewriting programs, stored procedures, or triggers, and database and data file modifications or conversions.

g. Provide analysis and programming services to identify and resolve problems or inefficiencies in existing related databases, files, and operational on-line or batch programs, including problem analysis, systems analysis, program modifications, changing help screens, rewriting programs, stored procedures or triggers, and database and data file modifications or conversions.

h. Provide maintenance of applications based on analysis of end-user evaluation of current system components.

i. Provide documentation and input to facilitate security certification including security configurations and change management configurations.

j. Utilize Agile-based methodologies. Note, O&M activity schedule is (up to) bi-monthly sprints for O&M requirements.

k. Provide development and integration testing and quality assurance, as necessary, to correct test problem reports.

l. Provide programming support, as necessary, to correct OPRs.

m. Test all modifications against external interfaces, validate, and provide test reports.

n. Maintain requirements traceability, modify code, and test applications in conjunction with other related development or O&M efforts.

o. Coordinate closely with Government Program Managers, applicable Government employees, and other contractors to ensure success across projects, stakeholders, sister organizations, and other network personnel.

p. Perform project technical compliance reviews including new software/hardware capabilities to determine if it meets security, network configurations within BEMSD IT services as requested by the Government.

q. Provide database administrators, as required, for application support.

r. Provide emergency and routine patching/release O&M.

s. Develop emergency back-out plan in conjunction with an emergency and routine fix/patch and execute plan if needed.

t. Provide timely impact analysis of change request and trouble reports that originate in both the operations and development environments in accordance with the approved PMP, CMP, and SDP.

u. Develop and execute current operational acceptance criteria to evaluate production acceptance of system releases.

v. Perform pre-deployment evaluation reviews to determine if system releases meet defined operational acceptance criteria.

w. Perform post-deployment evaluation reviews to determine if system releases meet defined operational acceptance criteria.

C.5.6.2 SUBTASK 6.2 – PROVIDE BEMSD LAB PRODUCTION O&M

The contractor shall provide development, technology assessments and testing, deployment and operations and maintenance of systems and equipment at and managed by a physical on-site lab at a Government location in VT. Similar functions may also be provided at other BEMSD locations, as directed by the Government. The lab allows for real-time analysis, classification, and aggregate display of surveillance events. The contractor shall provide the design, documentation, development, testing, and maintenance of systems/applications for tracking Agent activity and safety. Additionally, the contractor shall identify and document user and technical requirements, and develop surveillance components, systems, and applications including, but not limited to, the following:

a. Field surveillance processors/controllers services.
b. Field analysis/fusion processors.
c. Field database/web servers.
d. Field data services.
e. Central processors.
f. Central database/web servers.
g. Central data/report services.

The contractor shall maintain lab scalability for the ICAD application and provide testing and integration of surveillance hardware components including, but not limited to, sensor systems, camera systems, and biometric software/hardware.

Specifically, the contractor shall:

a. Assist CBP/OIT personnel in preparation, logistics, and deployment of field servers and workstations in support of surveillance operations.
b. Assist CBP/OIT personnel with identifying, troubleshooting, and resolving network problems negatively impacting real-time communications.
c. Assist CBP/OIT personnel in the modification of CBP-base system images and security policies for compatibility with mission critical system applications.
d. Assist CBP/OIT personnel in security review processes and certifications.
e. Assist CBP in implementing tactical command and control solutions in support of special operations.
f. Conduct remote backups of field data stores for storage.
g. Provide O&M IT sustainment functions for sensors, viewers, components, readers, and other physical supporting hardware for applications within the BEMSD IT portfolio.

C.5.7 TASK 7 – PROVIDE CUSTOMER SERVICE

The contractor shall provide customer service for BEMSD application customers including training and change management, customer outreach and communication, end-user help services, and knowledge management. The contractor shall support customers and the larger CBP OIT help desk, ensuring high levels of customer satisfaction.

C.5.7.1 SUBTASK 7.1 – PROVIDE END-USER PROBLEM-SOLVING SERVICES

The BEMSD IT portfolio is made up of multiple customer service functions and multiple entry points, and lacks consistent ticket visibility, status, and logging of resolutions. BEMSD is seeking a standardized approach to customer service and problem management through best practices including proactive analysis of tickets and improved visibility across applications.

The Field Support Directorate (FSD) within CBP OIT provides the Technology Service Desk (TSD), which uses Remedy and serves as the primary Tier 1 service desk for most CBP OIT functions. TSD receives service calls for most CBP OIT applications and systems, but it is only equipped to resolve basic issues. TSD logs tickets and assigns them to the appropriate application support teams for issues that cannot be resolved by the TSD. BEAGLE customer support is responsible for any issues not resolved by the TSD. If the BEAGLE contractor receives a service request outside of the TSD business process (ex. a call, email, or walk-up request) that has not already been logged in the Remedy ticket management system, the contractor shall create a ticket in Remedy to track the service request. The current application problem (i.e., help desk) volume across the BEMSD IT portfolio is provided as a document in the Electronic Reading Room (eRR) (Section J, Attachment I). The historical ticket volume is not necessarily an indication of future requirements.

The contractor shall provide customer service support for applications during “core hours”, which are defined as 6:00 a.m. until 6:00 p.m. Eastern Time, Monday through Friday. The CBP/OIT Emergency Operations Center runs the 24x7x365 Network Operations Center (NOC) and will escalate after-hours tickets to the appropriate BEMSD application POC. The BEAGLE contractor shall provide 24x7x365 escalation response services to BEMSD applications via on-call resources to address outages, significant performance degradations, and/or patch verifications during non-core hours. Similarly, as emergencies, incidents, or major operations

may arise, the contractor shall provide after-hours services to ensure application availability and functionality. Such notice for after-hours support will come from the FEDSIM COR, BEMSD TPOC, or appropriate BEMSD application POC.

Upon receipt of a customer's trouble-call, the contractor shall provide a standardized approach to resolve the problem including:

a. Opening a ticket in Remedy;

b. Performing a remediation assessment;

c. Answering the question, using remote access to troubleshoot, isolate, and resolve the problem, and enter into Remedy; or

d. Referring to the next tier level of help.

Contractor customer service personnel shall respond to issues affecting Mission Critical applications within ten minutes of contact, Mission Essential applications within 30 minutes of contact, and Mission Relevant applications within one hour of contact. Applications and their associated criticality levels are defined in the BEMSD Incident Classification Guide, which is provided in the eRR. The contractor shall report through TO management personnel the general description of the analysis and cause of the issue in a time commensurate with the incident classification, workarounds of the issue, as well as estimated timelines for returning to normal operations. **Note that the contractor shall provide service activities for both O&M as well as newly deployed systems, functionality and applications, which may occur outside of normal business hours.**

The contractor shall respond to requests for Operational Problem Reports (OPRs) from the Government, and shall resolve system failures or outages or any issues that will cause a system failure or outage within four hours or in accordance with application criticality (e.g., Intelligent Computer Assisted Detection (ICAD) within one hour). When the application is live and degradation or an outage occurs, the contractor shall develop an initial duty officer report followed by an After Action Report (AAR) including an RCA. The contractor must respond to and resolve help desk tickets pursuant to the operational impact provided by an end user and within the scope of their assigned tasks.

The contractor shall perform predictive analysis to anticipate changes in call volume (i.e., major evolution of software or new deployments), and perform RCAs to determine the cause of ticket volume spikes for applications as well as plan a course of action to address those root cause. The contractor shall provide daily ticket queues and Very Important Person (VIP) status to Government customer service leads via dashboard, email updates, TO management personnel, and in-person where required.

C.5.7.2 SUBTASK 7.2 – PROVIDE CUSTOMER COMMUNICATION, AND TRAINING

BEMSD provides full system and application development and maintenance services to a broad set of customers and end-users, both within and external to CBP. BEMSD requires contractor services that provide consistent communications and messaging coordinated through the designated BEMSD branch POC, and in accordance with the contractor's communications plan. A communications plan is required as part of the PMP (See Section C.5.1.5).

Customer communications are included as part of overall customer service. These communications include face-to-face, telephonic, videoconference, email, and/or a combination of all of these, and may require long-distance travel. Communications may entail participation in daily stand-up meetings, providing status or updates, customer outreach, and may require the contractor to provide oral presentations and participate in presentation events to CBP, other Government users, and the public.

To support new capabilities and the delivery of new functionality and updates, the contractor shall prepare on-line systems help, as required, and facilitate or participate in system design walk-throughs with key customer personnel, designated by the BEMSD TPOC to ensure design consistency and completeness. In addition, the contractor shall develop training materials for teaching users train-the-trainer methodologies, identify and analyze user pain points, and develop self-help, Frequently Asked Questions (FAQs), and other artifacts.

C.5.7.3 SUBTASK 7.3 – PROVIDE KNOWLEDGE MANAGEMENT

Knowledge management is essential to the identification, maintenance, and management of data, information, and knowledge utilized in support of services provided by BEMSD applications to end-users, internal BEMSD teams, and stakeholders. Knowledge management should provide BEMSD with a centralized mechanism to institutionalize initiatives, processes, approaches, policies, and systems that sustain and enhance the storage, assessment, sharing, refinement, and creation of knowledge and supporting materials.

The contractor shall leverage knowledge management to help promulgate consistent versions of plans and processes across BEMSD. The contractor shall develop robust knowledge management capabilities and artifacts in order to create awareness of capabilities that are in development and those already fielded. The contractor's knowledge management program shall provide for enabled collaboration, updated SOPs content management, records management, and business process management. The contractor shall provide standardized structures (taxonomies) for tagging content. The contractor shall provide appropriate individual, role-based access control. The contractor shall store and organize content in a way that it can be efficiently searched and shall perform analysis and trending of issues for visibility across the BEMSD enterprise.

As part of knowledge management, the contractor shall maintain a TO Documentation Library on CBP's instance of SharePoint or other Government-approved collaboration tools. This shall be the primary reference tool for the latest versions of:

a. Standard Operating Procedures (SOPs).

b. Configuration and architecture documentation.

c. TO governance documents and deliverables, such as the PMP, IMS, project overviews, assignment and POC lists, agendas and summaries of meetings and conferences, and other relevant documents. Deliverables containing contractor cost and financial data shall not be posted in the TO Document Library, but shall be delivered to the COR IAW the TO.

The TO Documentation Library shall be the reference tool for approved deliverables and other documentation indicated above. All TO deliverables shall be submitted as indicated in Section F.6 and as indicated in the Deliverables table in Section F.3 (referencing the corresponding TOR section).

C.5.8 TASK 8 – PROVIDE DATA ANALYSIS, RATIONALIZATION, AND ANALYTICS

The contractor shall provide a variety of analytics services expertise in order to gather, conceptualize, and prioritize the needs of its customers in a form that is most meaningful to begin successful architecture. The contractor shall utilize Business Intelligence tools, methodology, and expertise that assists in detecting trends, patterns, and non-obvious relationships in data contained in a multitude of systems and an enterprise data warehouse.

The contractor shall evaluate existing BEMSD data and reporting architecture and take strategic steps to enable a modern Business Intelligence gateway. Such tools for data extraction and analysis may, as appropriate, be built into application to provide analysts with the necessary data to respond rapidly to operational challenges. This effort may include establishing new integration points and potentially adding infrastructure. This effort will require the use of gathered expertise on available system data across BEMSD, data warehouse source data, and existing software and infrastructure. The contractor shall create both a short-term and long-term data strategy to focus this effort.

The contractor shall provide expertise and innovation utilizing (but not limited to) the following methods and tools to develop intelligence assets and processes that will drive operational outcomes at CBP. Where applicable, the contractor shall develop the use of artificial intelligence capabilities and advanced data analytics to enhance decision-making and improve border enforcement and mission support outcomes in the following areas:

a. **Statistical analysis** – modeling and statistical tools that can help analysts discover patterns or generalizations in the data. This analysis can produce models that can be used to identify similar patterns in other data or common characteristics among seemingly disparate data.
b. **Geospatial analysis** – visualization tools that can display a set of events or activities on a map showing streets, buildings, geopolitical borders, or terrain. This analysis can help produce intelligence about the location or type of location that is favorable for a particular activity.
c. **Link analysis** – visualization tools that can help analysts discover patterns of associations among various entities. This can produce a social network representation of the data.
d. **Temporal analysis** – visualization tools that can display events or activities in a timeline to help an analyst identify patterns or associations in the data. This can produce a time sequence.
e. **Machine Learning** – data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns, and make decisions with minimal human intervention.
f. **Predictive analysis** – analysis that uses data to make predictions about unknown future events. Predictive analytics uses many techniques from data mining, statistics, modeling, machine learning, and artificial intelligence to analyze current data to make predictions about future.

g. **Artificial Intelligence** – the simulation of human intelligence processes by computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions), and self-correction.
h. **Analytics as a Service (AaaS)** – the provisioning of analytics software and operations through web-delivered technologies.
i. **Extract Transfer Load (ETL) as a service** – the optimization of data schema structural mapping in order to enable automatic data integration.

The contractor shall produce ad hoc reports as required, including responses to data calls from BEMSD, CBP, and other Government entities. This includes analytics, audit support, as well as financial activities such as year-end closeouts.

C.5.9 TASK 9 – PROVIDE SOLUTIONS FOR THE EVOLUTION OF BEMSD BORDER SECURITY INITIATIVES (OPTIONAL)

The BEMSD organization and the BEAGLE TO have responsibility for providing rapid responses to the dynamic CBP and DHS-enterprise mission requirements as they arise and in response to domestic and global events. The contractor shall develop solutions for the implementation of new policy, executive orders, initiatives, and event objectives within the existing BEMSD portfolio, as described in Tasks 1 through 8. Additional as-needed requirements are variable in length and level of effort. Task 9 requirements and deliverables are described in Tasks 1 through 8, are within the scope of this TO, and may require additional personnel to meet the requirement.

This page intentionally left blank.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the FEDSIM COR and BEMSD TPOC at BEMSD locations.

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and BEMSD TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

E.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The FEDSIM CO or FEDSIM COR will provide written notification of acceptance or rejection (Section J, Attachment H) of all final deliverables within 15 workdays (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated impact to the award fee earned.

F.1 PERIOD OF PERFORMANCE

The period of performance will be a one year base period, and four one-year option periods. If the award of this TO does not occur prior to the end of FY2019, the Government will exercise Option Period 1 early such that it begins prior to the end of FY2020. All subsequent Option Periods will be sequential and will not overlap.

Base Period:	PS (Project Start) – 12 months from PS
Option Period 1:	September 30, 2020 – September 29, 2021
Option Period 2:	September 30, 2021 – September 29, 2022
Option Period 3:	September 30, 2022 – September 29, 2023
Option Period 4:	September 30, 2023 – September 29, 2024

F.2 PLACE OF PERFORMANCE

The duty station is defined as the authorized place of performance for the work of this TO. The primary Places of Performance are currently located in Williston, VT (ICAD program facility and lab), Alexandria, VA (Walker Lane) and Falls Church, VA. Occasional/ad-hoc telework is permissible through coordination with Government program leads.

In January 2021 - date subject to change - CBP OIT plans to relocate several National Capital Region operations to Ashburn, VA. The Government anticipates having a total of 426 seats (subject to change) available at the Ashburn facility for Government and contractor staff within the BEMSD organization.

Within 30 calendar days of the formal announcement of the move to Ashburn by CBP leadership, the contractor shall provide a Draft Ashburn Transition Plan (Section F, Deliverable 32) that details critical TO operational impacts and logistics of the move, including (but not limited to) timeline of relocating contractor personnel, outlining seating arrangements, identifying risks and proposed mitigation plans, and other important Government decisions that require attention connected to the move. A final plan shall be delivered after Government comments.

During the performance of the TO, the Government may require the contractor to identify a contractor-owned or leased facility within ten (10) miles of the CBP OIT Ashburn facility in order to accommodate contractor staff. If this becomes a requirement, the FEDSIM CO will notify the TO Program Manager in writing with adequate lead time.

Long distance travel is anticipated to be required in support of this effort.

F.3 TASK ORDER SCHEDULE AND MILESTONE DATES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

DEL: Deliverable
IAW: In Accordance With
NLT: No Later Than

TOA: Task Order Award

All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

Data Rights Clause - Abbreviations in the Gov't Rights column of the table below shall be interpreted as follows:

UR: Unlimited Rights, per FAR 27.404-1(a) and 52.227-14

RS: Restricted Software, per FAR 27.404-2 and 52.227-14

LD: Limited Rights Data, per FAR 27.404-2 and 52.227-14

SW: Special Works, per FAR 27.405-1 and 52.227-17

For software or documents that may be either proprietary COTS or custom, RS/LD rights apply to proprietary COTS software or documents and UR rights apply to custom software or documents. The Government asserts UR rights to open source COTS software. Any collateral agreements (within the meaning of FAR 52.227-14) proposed for data, regardless of the type of rights offered, shall be subject to the requirements of TOR Section H.13.1 and H.13.2. For purposes of the foregoing, the terms "collateral agreement," "Supplier Agreement," and "Commercial Supplier Agreement" have the same meaning.

The Government does not assert any rights to management software tools if the contractor does not plan to charge the Government directly for that tool and does not propose that the Government will own or use that tool.

The contractor shall deliver the deliverables listed in the following table on the dates specified. . The contractor shall provide the applicable data rights clause for each deliverable submitted:

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
01	Project Start (PS)	0001	C.5.1.2	At TOA plus 10 days	N/A
02	Kick-Off Meeting Agenda (to include Kick-Off Meeting slides)	0001	C.5.1.1	At least three days prior to the Kick-Off Meeting	UR
03	Kick-Off Meeting	0001	C.5.1.1	Within 5 days of PS	N/A
04	Kick-Off Meeting Minutes Report	0001	C.5.1.1	Within 3 days of Kick-Off Meeting	UR

05	Monthly Status Report (MSR)	X001	C.5.1.3	Monthly – 10th calendar day of the next month (or following business day)	UR
06	Monthly Technical Status Meeting	X001	C.5.1.3	Monthly (recurring date to be established with Government at Kick-Off Meeting)	UR
07	Monthly Technical Status Meeting Minutes	X001	C.5.1.3	Within 3 days of meeting	UR
08	Quarterly Program Management Review (PMR)	X001	C.5.1.4	Quarterly, beginning NLT 120 days after PS	UR
09	Quarterly Program Management Review (PMR) Minutes	X001	C.5.1.4	Within 3 days of meeting	UR
10	Project Management Plan and Updates (including QMP)	X001	C.5.1.5	Draft: Due at Kick-Off Meeting Final: Due 10 days after receipt of Government comments Updates: As project changes occur, no less frequently than annually	UR
11	Integrated Master Schedule and Updates (IMS)	X001	C.5.1.5	Draft: Due at Kick-Off Meeting Final Template: Due 10 days after receipt of Government comments Updates: Due monthly on the 10th calendar day of the next month (or following business day)	UR
12	Trip Reports	X001	C.5.1.7	Within 7 days of completing travel	UR
13	Transition-In Plan	0001	C.5.2.1	Updated Draft: Due at Kick-Off Meeting Final: Due 10 days after receipt of Government comments	UR
14	Transition-Out Plan	X001	C.5.2.2	Draft: Within six months of Project Start Final: Due 10 days after receipt of Government comments	UR
15	Proposed Innovation Projects	X001	C.5.3.3	As the contractor identifies potential innovation projects	UR

16	Innovation Project Implementation Plan	X001	C.5.3.3	Within 30 days of Government approval of a Proposed Innovation Project	UR
17	Service Level Agreements (SLAs)	X001	C.5.1.5	Draft: Within 5 days of PS (delivered as part of draft PMP, Deliverable 10) Final: Delivered with final PMP Revised SLAs: No fewer than 30 calendar days prior to start of next Award Fee Period (as appropriate). Approved changes shall be incorporated into updated PMP.	UR
18	Acquisition Risk Questionnaire	0001	C.5.1.1	Submitted at Kick-Off Meeting	UR
19	TO Budgetary ROM	X001	C.5.1.2	No fewer than 120 calendar days prior to start of next Option Period. Base Period ROM shall be delivered within 45 calendar days of Project Start.	UR
20	Application Migration Plan	X001	C.5.4.1	As directed by FEDSIM COR and BEMSD TPOC.	UR
21*+	Application Test Plans	X001	C.5.4.2	As appropriate or directed by the Government. Existing documentation shall be updated no less than annually.	UR
22*+	Software User Documentation	X001	C.5.4.2	As appropriate or directed by the Government. Existing documentation shall be updated no less than annually.	UR
23*+	Test Scripts	X001	C.5.4.2	As appropriate or directed by the Government. Existing documentation shall be updated no less than annually.	UR
24*	Architecture Artifacts and Roadmaps	X001	C.5.4.3	As directed by FEDSIM COR and BEMSD TPOC.	UR

25	Technology Integration Assessments and Impact Analyses	X001	C.5.4.3	As directed by FEDSIM COR and BEMSD TPOC.	UR
26	RESERVED				
27	Software Development Plan (SDP)	X001	C.5.5.1	Final: Within 10 days of receipt of Government comments on draft SDP. Updates: Periodically as DHS/CBP policies are updated or the contractor implements improved methodologies and/or procedures, but no less than annually.	UR
28	Requirements Traceability Matrix (RTM)	X001	C.5.5.2	As directed by FEDSIM COR and BEMSD TPOC.	UR
29	Configuration Management Plan (CMP), part of the SDP	X001	C.5.6.1	Within 10 days of receipt of Government comments on draft SDP. Updated in parallel with the SDP.	UR
30	Rough Order of Magnitude (ROM) Determinations for new application development	X001	C.5.5.2	As directed by FEDSIM COR and BEMSD TPOC.	UR
31	RESERVED				
32	Ashburn Transition Plan	X001	F.2	Draft: Within 30 calendar days of formal CBP announcement of move date to Ashburn, VA Final: Within 10 days of receipt of Government comments	UR
33	Redacted BEAGLE TO	X001	F.4	Within 10 days of execution of initial TO or any modification to the TO	N/A

***** Per agreement between the Mission Support Division (MSD) of BEMSD, the contractor, and FEDSIM, the following applications are exempted from these deliverables: (1) RevMod, (2)

Situation Management System (SMS), and (3) Facilities and Infrastructure Tracking Tool (FITT).

+ Per agreement with MSD and the Enforcement and Analytics Systems (EAS) Division of BEMSD, the contractor, and FEDSIM, the following applications are exempted from these deliverables: (1) SMART CM and (2) Remedy.

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14.

F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the FEDSIM CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a Portable Document Format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA (Section F, Deliverable 33). The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S. Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

a. Text	MS Word, Google Docs, PDF
b. Spreadsheets	MS Excel, Google Sheets
c. Briefings	MS PowerPoint, Google Slides
d. Drawings	MS Visio, Google Drawings
e. Schedules	MS Project, Smartsheet, or other Government-approved media

F.6 PLACE(S) OF DELIVERY

Copies of all deliverables shall be delivered to the FEDSIM COR at the following address:

GSA FAS AAS FEDSIM

ATTN: Tom White, COR (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (703) 589-2693
Email: tom.white@gsa.gov and BEAGLE.FEDSIM@gsa.gov

Copies of all deliverables shall also be delivered to the BEMSD TPOC. The DHS BEMSD TPOC name, address, and contact information will be provided at award.

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) (Section J, Attachment E) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)/ALTERNATE CONTRACTING OFFICER'S REPRESENTATIVE (ACOR)

The FEDSIM CO appointed a FEDSIM COR in writing through a COR Appointment Letter (Section J, Attachment A). The FEDSIM COR will receive, for the Government, all work called for by the TO and will represent the FEDSIM CO in the technical phases of the work. The FEDSIM COR will provide no supervisory or instructional assistance to contractor personnel.

The FEDSIM COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the FEDSIM CO by properly executed modifications to the Contract or the TO. The ACOR has the authority and responsibility to act as the COR only in the absence of the primary COR.

G.1.1 CONTRACT ADMINISTRATION

FEDSIM CO:

Aaron Sannutti
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 427-2513
Email: aaron.sannutti@gsa.gov

FEDSIM COR:

Tom White, COR (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (703) 589-2693
Email: tom.white@gsa.gov

FEDSIM ACOR:

Robert S. Hribar
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 501-1303
Email: robert.hribar@gsa.gov

FEDSIM ACOR:

Yusra Shah
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 213-0275
Email: Yusra.shah@gsa.gov

BEMSD TPOC:

BEMSD Technical Point of Contact (TPOC):

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

Task Order Number: *(from GSA Form 300, Block 2)*

Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*

FEDSIM Project Number: *(Fill in project number)*

Project Title: *(Fill in project title)*

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information SysTem (ASSIST) to submit invoices. The contractor shall manually enter CLIN charges into Central Invoice Services (CIS) in the ASSIST Portal. Summary charges on invoices shall match the charges listed in CIS for all CLINs. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned ID and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. The contractor shall provide invoice backup data, as an attachment to the invoice, in accordance with the contract type, including detail such as labor categories, rates, quantities of labor hours per labor category, and total cost by sub-CLIN. The FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment. A paper copy of the invoice is required for a credit.

The contractor is certifying, by submission of an invoice in the CIS, that the invoice is correct and proper for payment.

If there are any issues submitting an invoice, contact the Assisted Acquisition Services Business Systems (AASBS) Help Desk for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice backup in Excel to the FEDSIM COR and BEMSD TPOC for review prior to its submission to ASSIST. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9.

Each contract type shall be addressed separately in the invoice submission. Receipts shall be provided on an as requested basis.

The contractor shall submit invoices on a monthly basis for costs incurred. The contractor shall notify the FEDSIM COR if circumstances require the delay of invoices beyond one month.

The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following metadata:

a. GWAC Contract Number. .
b. TOA Number (NOT the Solicitation Number).
c. Contractor Invoice Number.
d. Contractor Name.
e. POC Information.
f. Current period of performance.
g. Amount of invoice that was subcontracted.

The amount of invoice that was subcontracted to a small business shall be made available upon request.

G.3.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice (all current charges shall be within the active period of performance) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees).
b. Employee company.
c. Exempt or non-exempt designation.
d. Employee Alliant 2 labor category.
e. Current monthly and total cumulative hours worked.
f. Direct Labor Rate.
g. Effective hourly rate (e.g., cumulative costs/cumulative hours).
h. Current approved billing rate percentages in support of costs billed.
i. Itemization of cost centers applied to each individual invoiced.
j. Itemized breakout of indirect costs (e.g., Fringe, Overhead (OH), General and Administrative (G&A) burdened costs for each individual invoiced (rollups are unacceptable)).
k. Any cost incurred not billed by CLIN (e.g., lagging costs).
l. Labor adjustments from any previous months (e.g., timesheet corrections).
m. Provide comments for deviation outside of standard monthly full time hours.

All cost presentations provided by the contractor in Excel shall show indirect charges itemized by individual with corresponding indirect rates with cost center information. The invoice detail shall be organized by CLIN.

The contractor may invoice for fee after accepting the modification which includes the award fee determination and any corresponding de-obligation of unearned fee. See the AFDP in Section J, Attachment D for additional information on the award fee determination process.

When the Incurred Cost method is used to determine the Award Fee Pool Allocation for an Award Fee period, the incurred cost shall be calculated using approved provisional billing rates as established by the cognizant Government auditor, in accordance with FAR 42.704. Approved provisional billing rates shall not be adjusted for the purpose of accumulating incurred costs and calculating the Award Fee Pool Allocation.

G.3.2 TOOLS AND OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the Tools and ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. Tools and/or ODCs purchased.
b. Request to Initiate Purchase (RIP) or Consent to Purchase (CTP) number or identifier.
c. Date accepted by the Government.
d. Associated CLIN.
e. Project-to-date totals by CLIN.
f. Cost incurred not billed by CLIN.
g. Remaining balance of the CLIN.

All cost presentations provided by the contractor shall also include OH charges, G&A charges and Fee in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

G.3.3 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulation (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Joint Travel Regulations (JTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR/DSSR. The invoice shall include the period of performance covered by the

invoice and the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request number or identifier, approver name, and approval date.
b. Current invoice period.
c. Names of persons traveling.
d. Number of travel days.
e. Dates of travel.
f. Number of days per diem charged.
g. Per diem rate used.
h. Total per diem charged.
i. Transportation costs.
j. Total charges.
k. Explanation of variances exceeding ten percent of the approved versus actual costs.
l. Indirect handling rate.

All cost presentations provided by the contractor shall also include OH charges and G&A charges in accordance with the contractor's DCAA cost disclosure statement.

G.4 TASK ORDER (TO) CLOSEOUT

The Government will unilaterally close out the TO NLT six years after the end of the TO period of performance if the contractor does not provide final DCAA rates by that time.

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO.

a. TOPM
b. Chief Engineer/Architect
c. Security Manager
d. Enforcement and Analytics Systems (EAS) Portfolio Manager
e. Border IT Systems (BITS) Portfolio Manager
f. Mission Support Division (MSD) Portfolio Manager
g. Web, Communications, and Research (WCR) Portfolio Manager

The Government desires that Key Personnel be assigned for the duration of the TO, and be located physically on Government site during business hours.

H.1.1 TOPM

The contractor shall identify a TOPM by name who shall provide management, direction, administration, quality assurance (as defined in Section C.5.1, and leadership of the execution of this TO). The TOPM shall serve as the contractor's single TO manager and shall be the contractor's authorized interface with the FEDSIM CO, FEDSIM COR, and BEMSD TPOC for the TO. The TOPM shall be authorized by the contractor's firm to make decisions and commit the contractor team in carrying out all aspects of the TO. The TOPM shall be available to plan, direct, communicate, and control the overall management and operational functions specified herein during normal hours of operation and during periods of no-notice emergencies. The TOPM must be employed by the BEAGLE prime contractor.

It is required that the TOPM has the following qualifications:

a. Possesses an active Project Management Professional certification (provide certification number) from the Project Management Institute (PMI).
b. At least ten years of experience managing programs in an IT environment.

It is desired that the PM has the following qualifications:

a. A Bachelor's degree in IT, Computer Science, Information Systems, or a related field.
b. Experience developing a strategic vision for a complex organization, balancing modernization needs with critical daily operations and maintenance requirements.
c. Experience managing programs or projects in a DHS environment.
d. Demonstrated experience in the successful delivery of similar programs and with organizing, directing, and managing contract operations involving multiple, complex, and interrelated project tasks.

H.1.2 CHIEF ENGINEER/ARCHITECT

The contractor shall provide a Chief Engineer/Architect to direct technical personnel and contractor project managers on the TO in the architecture and design of solutions to meet requirements and improve service. The Chief Engineer/Architect will also provide strategic and technical planning and oversight on migration of applications to the cloud.

It is required that the Chief Architect has the following qualifications:

a. Recognized cloud certification, such as Amazon Web Services (AWS) Certified Solutions Architect, Cloud Certified Professional.

It is desired that the Chief Architect has the following qualifications:

a. At least five years of experience with engineering/architecting enterprise IT applications.
b. Experience with leading migrations of applications and/or systems to the cloud.
c. Experience with mobile applications and data analytics.
d. A Bachelor's degree in IT, Computer Science, Information Systems, or a related field.
e. Experience with managing and consolidating diverse user interfaces and architectures within an application portfolio.
f. Experience providing detailed engineering and technical leadership to engineering staff involving multiple, complex, and interrelated project tasks.

H.1.3 SECURITY MANAGER

The contractor shall provide a Security Manager to oversee security compliance and processes on the TO, as well as direct contractor ISSOs. The Security Manager will be the primary liaison with the Government's security lead, and shall ensure that critical security functions such as ATOs, certificate renewals, and related tasks are completed successfully and on-schedule. The Security Manager shall ensure that security risks and findings are not only appropriately documented, but shall proactively provide potential solutions to remediate issues while allowing systems to remain operational and compliant in a mission-first environment.

It is required that the Security Manager has the following qualifications:

a. Possesses an active Certified Information Systems Security Manager (CISSM) or Certified Information Systems Security Professional (CISSP) certification.

It is desired that the Security Manager has the following qualifications:

a. At least five years of experience managing IT security teams in a Government environment.
b. A Bachelor's degree in IT, Computer Science, Information Systems, or a related field.
c. Demonstrated experience defining strategic governance for security management, defining quality metrics, and implementing repeatable processes for a portfolio of applications.

H.1.4 ENFORCEMENT AND ANALYTICS SYSTEMS (EAS) PORTFOLIO MANAGER

The contractor shall provide an EAS Portfolio Manager to oversee contractor staff working on applications and systems within the EAS division of BEMSD. The EAS Portfolio Manager shall be the primary liaison with the Government's EAS division director and shall provide strategic advice, planning, and guidance on maintaining, modernizing, and migrating applications and systems in the EAS portfolio.

It is required that the EAS Portfolio Manager has the following qualifications:

a. At least five years of experience managing teams in an IT environment.

It is desired that the EAS Portfolio Manager has the following qualifications:

a. Experience managing multiple software development teams concurrently in a Government organization.
b. Experience with Agile development methodology and SecDevOps .
c. At least ten years' experience managing teams similar in size and scope to the EAS portfolio of applications under this TO.
d. A Bachelor's degree in IT, Computer Science, Information Systems, or a related field.

H.1.5 BORDER IT SYSTEMS (BITS) PORTFOLIO MANAGER

The contractor shall provide a BITS Portfolio Manager to oversee contractor staff working on applications and systems within the BITS division of BEMSD. The BITS Portfolio Manager shall be the primary liaison with the Government's BITS division director and shall provide strategic advice, planning, and guidance on maintaining, modernizing, and migrating applications and systems in the BITS portfolio.

It is required that the BITS Portfolio Manager has the following qualifications:

a. At least five years of experience managing teams in an IT environment.

It is desired that the BITS Portfolio Manager has the following qualifications:

a. Experience managing multiple software development teams concurrently in a Government organization.
b. Experience with Agile development methodology and DevOps.
c. At least ten years' experience managing teams similar in size and scope to the BITS portfolio of applications under this TO.
d. A Bachelor's degree in IT, Computer Science, Information Systems, or a related field.

H.1.6 MISSION SUPPORT DIVISION (MSD) PORTFOLIO MANAGER

The contractor shall provide a MSD Portfolio Manager to oversee contractor staff working on applications and systems within the MSD division of BEMSD. The MSD Portfolio Manager shall be the primary liaison with the Government's MSD division director and shall provide strategic advice, planning, and guidance on maintaining, modernizing, and migrating applications and systems in the MSD portfolio.

It is required that the MSD Portfolio Manager has the following qualifications:

a. At least five years of experience managing teams in an IT environment.

It is desired that the MSD Portfolio Manager has the following qualifications:

a. Experience managing multiple software development teams concurrently in a Government organization.
b. Experience with Agile development methodology and SecDevOps.
c. Experience in directing large-scale COTS software implementations.
d. At least ten years' experience managing teams similar in size and scope to the MSD portfolio of applications under this TO.
e. A Bachelor's degree in IT, Computer Science, Information Systems, or a related field.

H.1.7 WEB, COMMUNICATIONS, AND RESEARCH (WCR) PORTFOLIO MANAGER

The contractor shall provide a WCR Portfolio Manager to oversee contractor staff working on applications and systems within the WCR division of BEMSD. The WCR Portfolio Manager shall be the primary liaison with the Government's WCR division director and shall provide strategic advice, planning, and guidance on maintaining, modernizing, and migrating applications and systems in the WCR portfolio.

It is required that the WCR Portfolio Manager has the following qualifications:

a. At least five years of experience managing teams in an IT environment.

It is desired that the WCR Portfolio Manager has the following qualifications:

a. Experience managing multiple software development teams concurrently in a Government organization.
b. Experience with Agile development methodology and SecDevOps.
c. Experience in directing Platform-as-a-Service (PaaS) and Customer Relationship Management (CRM) system implementations.
d. At least ten years' experience managing teams similar in size and scope to the WCR portfolio of applications under this TO.
e. A Bachelor's degree in IT, Computer Science, Information Systems, or a related field.

H.1.8 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the FEDSIM CO. Prior to utilizing other than the Key Personnel specified in its proposal in response to the TOR, the contractor shall notify the FEDSIM CO and the FEDSIM COR of the existing TO. This notification shall be NLT ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute Key Personnel qualifications shall be equal to, or greater than, those of the Key Personnel substituted. If the FEDSIM CO and the FEDSIM COR determine that a proposed substitute Key Personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination.

H.2 GOVERNMENT-FURNISHED PROPERTY (GFP)

The contractor shall institute property control and accountability procedures to safeguard and maintain all GFP, including Contractor Acquired Property (CAP), in accordance with FAR 52.245-1 and DHS 4300 A. The contractor shall report any loss or damage of Government Property to the BEMSD TPOC and the FEDSIM COR. The contractor shall submit a Full Incident Report for any loss and damages. All GFP shall be accounted for and signed for by a designated contractor employee at each performance site. These designated contractor personnel shall also be accountable for inventory requirements and loss of or damage to GFP in accordance with FAR 52.245-1, Government Property.

H.3 GOVERNMENT-FURNISHED INFORMATION (GFI)

The contractor shall use GFI, data, and documents only for the performance of work under this TO, and shall return all GFI, data, and documents to the Government at the end of the performance period. The contractor shall not release GFI, data, and documents to outside parties without the prior and explicit consent of the FEDSIM CO.

H.4 SECURITY

The contractor shall comply with the CBP administrative, physical, and technical security controls to ensure that the Government's security requirements are met. The contractor shall not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance under this TO.

H.4.1 CONTRACTOR PRE-SCREENING

Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to IT resources shall verify minimal suitability requirements, as described below, for all persons/candidates designated for employment under any CBP contract by pre-screening the person/candidate prior to submitting the name for consideration to work.

Pre-screening the candidate ensures that minimum suitability requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Candidates shall also be submitted for a financial background check. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:

a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self-certification, by public records check; or, if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontracts to initiate a drug testing program if they do not have one already in place.
c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self-certification, by public records check, or other reference checks conducted in the normal course of business.
d. Financial irresponsibility related to tax liens and bankruptcy within the last seven to ten years. An acceptable means of obtaining information related to financial irresponsibility is through a financial background check.

Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources.

Failure to comply with the pre-screening requirement will result in the FEDSIM CO taking the appropriate remedy.

H.4.2 CBP BACKGROUND INVESTIGATION (BI)

A BI is required for performance under this effort. Contractor employees and sub-contractors shall not begin working until, at a minimum, an interim or partial BI is approved by CBP. The citizenship requirements for accessing CBP systems and granting CBP BIs are outlined in CBP OIT Handbook 1400-05D, Section 4.1.1. Exceptions to this requirement, such as granting access to certain systems with a "limited" or "partial" BI, or authorizing work of any kind without a limited or partial BI, will be handled on a case-by-case basis, and access to facilities, systems, and data will be limited until the individual is cleared. Should clearance requirements beyond a CBP BI (e.g., Secret or Top Secret) be needed, a modification will be issued to add this requirement to the Key Personnel, or any contractor personnel, identified as needing such requirement.

All personnel employed by or sub-contracted to the contractor or responsible to the contractor for work performed hereunder shall either currently possess or be able to favorably pass a full BI as required by CBP policies and procedures prior to beginning work with CBP. This policy applies to any personnel who will perform work on this TO. Executive Order 13467 allows for the acceptance of "suitability reciprocity" to contractor personnel who are component employees within DHS.

Within five (5) business days after the contract kick-off meeting, the BEMSD BI Process Coordinator (BIPC) will send the blank BI forms to the TOPM. These forms, which comprise the "BI package", include:

- CBP Form 77 (Contractor Employee Initial Background Investigation);
- CBP Form 0078 (Background Investigation Requirements Document, or BIRD);
- Fair Credit Reporting Act (FCRA) form; and
- CBP Non-Disclosure Agreement (NDA) form.

The contractor TOPM (or designated contractor representative) is responsible for completing (pre-filling) sections on these forms that pertain to the contract, such as contract number, duty address, work phone numbers, and BEMSD TPOC name. The contractor is responsible for providing these forms to any new employees and sub-contractors proposed for this TO at any time throughout the period of performance of this TO for those individuals to complete the remainder of the information on the forms. After completion of the forms by the proposed contractor or sub-contractor, the TOPM shall review the package for completeness and forward the BI package to the BEMSD BIPC.

The BEMSD BIPC will review the submitted BI package for completeness and accuracy and will obtain the BEMSD TPOC's signature on the Form 77. Once signed, the BEMSD BIPC will submit the BI package to the CBP eQIP coordinator. The BEMSD BIPC will retain a copy of the package in an electronic filing system.

The eQIP coordinator will review the BI package for completeness. If there are errors or missing information, the application will be rejected and returned to the contractor employee BI candidate for revisions, with notifications going to the BEMSD TPOC, BEMSD BIPC, and TOPM (or their designated contractor representative). The BI candidate shall make the necessary

revisions and resubmit the BI package to the BEMSD BIPC to route back to the eQIP coordinator.

Once the eQIP coordinator determines that the BI package is error-free, and if the BI candidate holds a current clearance, the eQIP coordinator will work with CBP's Office of Professional Responsibility (OPR) to determine if the contractor BI candidate is reciprocity-eligible. If the candidate is eligible for reciprocity, the candidate and the TOPM will be notified, and no eQIP or fingerprint cards will be needed. The reciprocity eligibility process can take 30 days or more.

If no reciprocity exists, or the candidate is otherwise not eligible for consideration for reciprocity, the eQIP coordinator will send the contractor BI candidate an email requesting them to complete the eQIP application. At the same time, the eQIP coordinator will send the BI candidate a set of fingerprint cards (form FD-258) to be completed. The BI candidate can complete the fingerprint cards at a local police department or CBP badging office. The BI candidate is responsible for sending the fingerprint cards to the eQIP coordinator via tracked mail if they are not completed at a CBP badging office.

After receipt of the fingerprint cards, the eQIP coordinator will review the eQIP application. The application must be submitted no later than 30 days after the initial eQIP invite, or else it will be rejected. If the eQIP coordinator finds incomplete sections or errors, the eQIP application will be rejected back to the BI candidate to address (with notifications to the BEMSD TPOC, BEMSD BIPC, and TOPM). The BI candidate shall correct any errors or incomplete sections and resubmit the eQIP directly back to the eQIP coordinator in the eQIP system.

Once the eQIP coordinator has determined that the eQIP application is complete and error-free, the eQIP application and fingerprint cards will be sent to OPR for the BI process to begin. It can take up to three (3) months to obtain a limited or partial BI. The full BI clearance has historically averaged six (6) months; however, the full BI clearance can take up to 9-12 months depending on the candidate and the volume of BIs being processed. Failure of any contractor personnel to successfully pass a full BI shall be cause for the candidate's immediate dismissal from the project and replacement by a similar and equally qualified candidate. This policy also applies to any personnel hired as replacements during the term of the TO.

H.4.3 CLEARANCES

Contractor personnel under this TO require a CBP BI.

H.4.4 IDENTIFICATION BADGES

All contractor employees shall be required to wear CBP identification badges at all times when working in Government facilities.

H.4.5 PHYSICAL AND IT SECURITY REQUIREMENTS

The contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel shall be responsible for physical security of work areas and CBP furnished equipment issued under this contract.

The FEDSIM CO/COR may require the contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the FEDSIM CO.

The contractor shall ensure that its employees, who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.

Upon completion of this contract, the contractor shall return all sensitive information used in the performance of the contract to the BEMSD TPOC. The contractor shall certify, in writing, that all sensitive and non-public information has been purged from any contractor-owned system.

H.4.6 INFORMATION ASSURANCE

The contractor may have access to sensitive (including privileged and confidential) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

H.4.7 REMOTE ACCESS

Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or GFE.

H.4.8 HANDLING PERSONALLY IDENTIFIABLE INFORMATION (PII)

The contractor shall comply with the Privacy Act, CBP, and DHS privacy policies and procedures when handling PII. This includes reporting loss, theft, or unauthorized access to sensitive PII within one hour of discovery and reviewing contractor applicable policies at least annually.

H.4.9 SECURITY CLEARANCES

In general, all necessary facility and employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

H.4.10 SECURITY CONTROLS

a. The contractor shall comply with the U.S. CBP administrative, physical, and technical security controls to ensure that the Government's security requirements are met.
b. All GFE/GFI shall be protected to the degree and extent required by local rules, regulations, and procedures. The contractor shall comply with all security policies contained in CBP Handbook 1400-05D, Information Systems Security Policies and Procedures Handbook.

c. All services provided under this contract shall be compliant with the DHS information security policy identified in DHS Management Directive (MD) 4300.1, IT Systems Security Program and DHS 4300A, Sensitive Systems Handbook.
b. All contractor employees under this contract shall wear identification (ID) access badges when working in CBP facilities. Prior to contractor employees' departure/separation, all badges, building passes, parking permits, keys, and pass cards shall be given to the BEMSD TPOC.
c. All contractor employees shall be registered in the Contractor Tracking System (CTS) database. The contractor shall provide timely start information to the Government to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule, and contract-specific information. Government personnel shall provide the contractor with instructions for receipt of CTS registration information.
d. The contractor shall provide employee departure/separation dates to the BEMSD TPOC in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when Government personnel complete a contractor performance review or other performance-related measures

H.4.11 DHS SPECIAL CLAUSE - SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) Applicability. This clause applies to the contractor, its subcontractors, and contractor employees (hereafter referred to collectively as "contractor"). The contractor shall insert the substance of this clause in all subcontracts.

(b) Definitions. As used in this clause – "Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, SSN, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual. PII is a subset of sensitive information. Examples of PII include, but are not limited to, name, date of birth, mailing address, telephone number, SSN, email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual. "Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security

interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, U.S.C. (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the DHS (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the DHS (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures. "Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, contractor system, or sensitive information. "Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: SSN, driver's license or state ID number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)

(2) Date of birth (month, day, and year)

(3) Citizenship or immigration status

(4) Ethnic or religious affiliation

(5) Sexual orientation

(6) Criminal history

(7) Medical information

(8) System authentication information such as mother's maiden name, account passwords or PIN Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors or available upon request from the FEDSIM CO including, but not limited to, the following:

(1) DHS MD 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding SPII

(6) DHS Instruction Handbook 121-01-007 DHS Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required. (1) DHS policies and procedures on contractor personnel security requirements are set forth in various MDs, Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for IT resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 DHS Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the contractor except as specified in the contract.

(3) All contractor employees with access to sensitive information shall execute DHS Form 11000-6, DHS Non-Disclosure Agreement (NDA), as a condition of access to such information.

The contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The contractor shall provide copies of the signed NDA to the FEDSIM COR NLT two days after execution of the form.

(4) The contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the FEDSIM COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The contractor shall not input, store, process, output, and/or transmit sensitive information within a contractor IT system without an ATO signed by the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three years. The contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below. (1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates. (i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided RTM and Government security documentation templates. SA documentation consists of the following: SP, Contingency Plan, Contingency Plan Test Results, CMP, Security Assessment Plan, SAR, and ATO Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the contractor shall submit a signed SA package, validated by an independent third party, to the BEMSD TPOC for acceptance by the Headquarters or Component CIO, or designee, at least 30 days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the FEDSIM CO shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the contractor's responsibility to ensure the IT system controls are implemented and operating effectively. (ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. The contractor shall address all deficiencies before submitting the SA package to the Government for acceptance. (iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the contractor may be required to support the Government in the completion of the PTA. The requirement to complete the PTA is triggered by the creation, use, modification, upgrade, or disposition of a contractor IT system that will store, maintain and use PII, and must be renewed at least every three years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that PMPs and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about use, access, storage, and maintenance of PII on the

contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three years. The contractor is required to update its SA package as part of the ATO renewal process. The contractor shall update its SA package by one of the following methods:

(1) Updating the SA documentation in the DHS automated IA tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or

(2) Submitting an updated SA package directly to the BEMSD TPOC for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and, therefore, it is important that the contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The contractor shall, through the FEDSIM CO and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the FEDSIM CO may direct the contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the

sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the FEDSIM COR with requested information within three business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for contractor systems.

(f) Sensitive Information Incident Reporting Requirements

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the contractor shall also notify the FEDSIM CO, FEDSIM COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the FEDSIM CO's email address is not immediately available, the contractor shall contact the FEDSIM CO immediately after reporting the incident to the Headquarters or Component SOC. The contractor shall not include any sensitive information in the subject or body of any email. To transmit sensitive information, the contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report: (i) Data Universal Numbering System (DUNS). (ii) Contract numbers affected unless all contracts by the company are affected. (iii) Facility Commercial and Government Entity (CAGE) code if the location of the event is different than the prime contractor location. (iv) POC if different than the POC recorded in the System for Award Management (address, position, telephone, email). (v) FEDSIM CO POC (address, telephone, email). (vi) Contract clearance level. (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network. (viii) Government programs, platforms, or systems involved. (ix) Location(s) of incident. (x) Date and time the incident was discovered. (xi) Server names where sensitive information resided at the time of the incident, both at the contractor and subcontractor level.

(xii) Description of the Government PII and/or SPII contained within the system. (xiii) Number of people potentially affected and the estimated or actual number of records exposed and/or contained within the system. (xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the FEDSIM CO in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following: (i) Inspections, (ii) Investigations, (iii) Forensic reviews, and (iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements

(1) The contractor shall have in place procedures and the capability to notify any individual whose PII resided in the contractor IT system at the time of the sensitive information incident not later than five business days after being directed to notify individuals, unless otherwise approved by the FEDSIM CO. The method and content of any notification by the contractor shall be coordinated with, and subject to prior written approval by the FEDSIM CO, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The contractor shall not proceed with notification unless the FEDSIM CO, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the contractor's use of address verification and/or address location services. At a minimum, the notification shall include: (i) A brief description of the incident. (ii) A description of the types of PII and SPII involved. (iii) A statement as to whether the PII or SPII was encrypted or protected by other means.

(iv) Steps individuals may take to protect themselves. (v) What the contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents. (vi) Information identifying who individuals may contact for additional information. (i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the contractor may be required to, as directed by the FEDSIM CO: (1) Provide notification to affected individuals as described above; and/or (2) Provide credit monitoring services to individuals whose data was under the control of the contractor or resided in the contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the contractor has no affiliation. At a minimum, credit monitoring services shall include: (i) Triple credit bureau monitoring. (ii) Daily customer service. (iii) Alerts provided to the

individual for changes and fraud. (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(3) Establish a dedicated call center. Call center services shall include: (i) A dedicated telephone number to contact customer service within a fixed period. (ii) Information necessary for registrants/enrollees to access credit reports and credit scores. (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics. (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate. (v) Customized FAQs, approved in writing by the FEDSIM CO in coordination with the Headquarters or Component Chief Privacy Officer. (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the contractor shall submit the certification to the COR and the CO following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

H.4.12 DHS SPECIAL CLAUSE - IT SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) Applicability. This clause applies to the contractor, its subcontractors, and contractor employees (hereafter referred to collectively as "contractor"). The contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The DHS requires that contractor employees take an annual IT Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-trainingrequirements-contractors. The contractor shall maintain copies of training certificates for all contractor and subcontractor employees as a record of compliance. The contractor shall notify the FEDSIM COR when the training has been completed. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the FEDSIM COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS IT resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information.

The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-andtraining-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within 30 days of contract award. Any new contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The contractor shall maintain signed copies of the DHS Rules of Behavior for all contractor and subcontractor employees as a record of compliance. The contractor shall notify the FEDSIM COR that the DHS Rules of Behavior have been signed by each employee not later than 30 days after contract award. The DHS Rules of Behavior will be reviewed annually and the FEDSIM COR will provide notification when a review is required.

(c) Privacy Training Requirements. All contractor and subcontractor employees that will have access to PII and/or SPII are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-securityand-training-requirements-contractors. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The contractor shall maintain copies of training certificates for all contractor and subcontractor employees as a record of compliance. The contractor shall notify the FEDSIM COR that the training has been completed by all applicable employees not later than 30 days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the FEDSIM COR via e-mail notification not later than October 31st of each year. The email notification shall state the required training has been completed for all contractor and subcontractor employees.

H.5 UNIQUE STANDARDS

H.5.1 CBP EA COMPLIANCE

The contractor shall ensure that the design conforms to the DHS and CBP EA, the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO), and Chief Architects (CA).

The contractor shall conform to the Federal EA (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the contractor shall use DHS/CBP approved products, standards, services, and profiles, as reflected by the hardware, software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software, or infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process (including a trade study with no All developed solutions shall be compliant with the Homeland Security (HLS) EA.

All IT hardware and software shall be compliant with the HLS EA. Compliance with the HLS EA shall be derived from and aligned through the CBP EA. Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and EA Information Repository.

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

H.5.2 SECURITY POLICY REQUIREMENT

All hardware, software, and services provided under this TO must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

H.5.3 ENCRYPTION COMPLIANCE REQUIREMENT

a. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
b. National Security Agency (NSA) Type 2 or Type 1 encryption.
c. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the DHS IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

H.5.4 PERSONAL IDENTIFICATION VERIFICATION (PIV) CREDENTIAL COMPLIANCE

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

H.6 APPLICABLE DOCUMENTS

The contractor shall adhere to the following policies, standards, directives, processes, and

procedures in performing work under this TO:

a. DHS Sensitive Systems Handbook policy 4300A, Version 13.1, July 27, 2017, or current version.
b. DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018 or current version.
c. Information Systems Security and Procedures Handbook, CIS HB 1400-05D.
d. CBP OIT Change Management Handbook.
e. DHS Systems Engineering Lifecycle, Instruction Number 102-01-103, November 5, 2015 or current version.
f. Information Technology Infrastructure Library (ITIL) Standards.
g. Security Engineering Branch (SEB) Escalation Procedure.
h. CBP TRM.
i. CBP EA.
j. DHS Data Management Policy MD 103-01.
k. Enterprise Data Management and Engineering Directorate (EDMED) Change Control Tool.
l. OIT 2018 Strategic Plan.

H.7 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.7.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the FEDSIM CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.
b. The contractor is required to complete and sign an OCI Statement (Section J, Attachment K). The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.
c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.
d. In addition to the mitigation plan, the FEDSIM CO may require further information from the contractor. The FEDSIM CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.
e. If any such conflict of interest is found to exist, the FEDSIM CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award.

Alternatively, the FEDSIM CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

H.7.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (Section J, Attachment L) and ensure that all its personnel (including subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.
b. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained from the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.8 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

H.9 ADEQUATE COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and Contract performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the Contract.

H.10 APPROVED PURCHASING SYSTEM

The objective of a contractor purchasing system assessment is to confirm it is a Government-approved purchasing system and evaluate the efficiency and effectiveness with which the

contractor spends Government funds and complies with Government policy with subcontracting. A Government-audited and approved purchasing system (e.g., approved by DCAA or Defense Contract Management Agency (DCMA)) is mandatory.

When reviews are conducted of the purchasing system during the performance of the TO, the contractor shall provide the results of the review to the FEDSIM CO within ten workdays from the date the results are known to the contractor.

H.11 TRAVEL

H.11.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. FTR - prescribed by the GSA, for travel in the contiguous U.S.
b. JTR, Volume 2, DoD Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. DSSR (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.11.2 TRAVEL AUTHORIZATION REQUESTS (TAR)

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a TAR (Section J, Attachment M) for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR or JTR. All travel requests (TARs) and approvals shall be done via CBP BEMSD's OT&T application within Salesforce.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a description of the travel proposed including a statement as to purpose.
c. Be summarized by traveler.
d. Identify the TO number.
e. Identify the CLIN associated with the travel.
f. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.12 TOOLS (HARDWARE/SOFTWARE) AND/OR ODCs

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the

Government or the contractor. If the contractor initiates a purchase within the scope of this TO , the contractor shall submit to the FEDSIM COR a Request to Initiate Purchase (RIP) (Section J, Attachment N. If the prime contractor is to lose an approved purchasing system, the contractor shall submit to the FEDSIM CO a Consent to Purchase (CTP) (Section J, Attachment O. The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the FEDSIM COR or an approved CTP from the FEDSIM CO and without complying with the requirements of Section H.13.2

H.13 COMMERCIAL SUPPLIER AGREEMENTS

H.13.1 The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in Section C and as contemplated in the Tools and ODC CLINs in Section B, may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as “clickwrap” or “browsewrap” (collectively, “Supplier Agreements”). For purposes of this TO, the Supplier Agreements are “collateral agreements” within the meaning of the FAR clause at 52.227-14.

H.13.2 The contractor shall ensure that any proposed Supplier Agreements allow the associated software and services to be used as necessary to achieve the objectives of this TO. The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO prior to purchase and shall cooperate with the Government, including negotiations with the licensor as appropriate, to ensure compliance with this Section. Without limiting the generality of the foregoing, a compliant Supplier Agreement shall permit all of the following at no extra charge to the Government: (a) access and use by support contractors, including a successor contractor upon termination or expiration of this TO; (b) access and use by employees of other Federal, state, and local law enforcement agencies; (c) transfer to a different data center and/or a successor contractor’s cloud; and (d) the creation of derivative works that shall be subject to at least the same rights as set forth in subparagraphs (a) through (c) above. The above rights constitute “other rights and limitations” as contemplated in subparagraph (d) of the FAR clause at 52.227-14, Rights In Data – General (May 2014), Alternate III (Dec 2007).

H.14 PRESS/NEWS RELEASE

The contractor shall not make any press/news release pertaining to this procurement without prior Government approval and only in coordination with the FEDSIM CO.

H.15 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application, or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

H.16 INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

All contractor employees using DHS information systems or processing DHS data shall be required to receive Security Awareness Training. This training will be provided by the appropriate component agency of DHS.

Contractors, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of DHS, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. DHS contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access DHS information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or ISSO.

The following trainings are mandatory for all contractor employees on this TO:

Training Name	Frequency	Method of Delivery
CBP Suicide Prevention	Annual	Performance and Learning Management System (PALMS)
DHS Insider Threat Training	Annual	PALMS
CBP Cyber Security Awareness and Rules of Behavior Training	Annual	PALMS
Preventing and Addressing Workplace Harassment	Annual	PALMS
CBP Annual Integrity Awareness Training	Annual	PALMS
Privacy at DHS: Protecting Personal Information	Annual	PALMS
Counterintelligence Awareness Web-Based Training	Bi-annual (every two years)	PALMS
Basic Records Management	One Time (within 30 days of entry on duty)	PALMS

H.17 AWARD FEE

See the AFDP in Section J, Attachment D.

I.1 TASK ORDER CLAUSES

All applicable and required clauses set forth in FAR 52.301 automatically flow down to all Alliant 2 TOs, based on their specific contract type (e.g., cost, fixed-price, etc.), statement of work, competition requirements, commercial or not commercial, and dollar value as of the date the TO solicitation is issued.

I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the FEDSIM CO will make their full text available. Also, the full text of a clause may be accessed electronically at the FAR website:

http://www.acquisition.gov/far/

FAR	TITLE	DATE
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2016
52.203-14	Display of Hotline Poster(s)(https://www.oig.dhs.gov/hotline)	OCT 2016
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	APR 2014
52.204-2	Security Requirements	AUG 1996
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2016
52.204-13	System for Award Management Maintenance	OCT 2018
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	JUL 2018
52.215-21	Requirements for Certified Cost or Pricing Data and Data Other than Certified Cost or Pricing Data—Modifications	OCT 2010
52.215-23	Limitations on Pass-Through Charges	OCT 2009
52.216-7	Allowable Cost and Payment Fill-in: 30 days	JUN 2013
52.219-8	Utilization of Small Business Concerns	NOV 2016
52.219-9	Small Business Subcontracting Plan	JAN 2017
52.223-15	Energy Efficiency in Energy Consuming Products	DEC 2007
52.223-16	Acquisition of EPEAT®-Registered Personal Computer Products	OCT 2015
52.224-1	Privacy Act Notification	APR 1984

FAR	TITLE	DATE
52.224-2	Privacy Act	APR 1984
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.225-25	Prohibition on Contracting With Entities Engaging in Certain Activities or Transactions Relating to Iran—Representations and Certifications	OCT 2015
52.227-14	Rights in Data – General	MAY 2014
52.227-14	Rights In Data –Alternate II	DEC 2007
52.227-14	Rights In Data –Alternate III	DEC 2007
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	DEC 2007
52.227-17	Rights In Data Special Works	DEC 2007
52.227-21	Technical Data Declaration Revision and Withholding of Payment – Major Systems	MAY 2014
52.232-18	Availability of Funds	APR 1984
52.232-20	Limitation of Cost	APR 1984
52.232-22	Limitation of Funds	APR 1984
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.237-3	Continuity of Services	JAN 1991
52.239-1	Privacy or Security Safeguards	AUG 1996
52.244-6	Subcontracts for Commercial Items	JAN 2017
52.245-1	Government Property	JAN 2017
52.246-5	Inspection of Services—Cost-Reimbursement	APR 1984
52.246-25	Limitation of Liability – Services	FEB 1997
52.247-67	Submission of Transportation Documents for Audit Fill-in: COR, see Section G	FEB 2006
52.249-6	Termination (Cost-Reimbursement)	MAY 2004
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012

I.2.1 FAR CLAUSES INCORPORATED BY FULL TEXT

52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILANCE SERVICES OR EQUIPMENT (AUG 2020)

(a) *Definitions.* As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (*e.g.*, connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (*e.g.*, fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (*e.g.*, connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (*e.g.*, voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition*.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of the end of the period of performance.

(End of clause)

FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

a. The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.
b. If the Government exercises this option, the extended contract shall be considered to include this option clause.
c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

(End of clause)

I.3 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at the GSAM website:

https://www.acquisition.gov/gsam/gsam.html/

GSAM	TITLE	DATE
552.204-9	Personal Identity Verification Requirements	OCT 2012
552.232-25	Prompt Payment	NOV 2009
552.232-39	Unenforceability of Unauthorized Obligations (FAR Deviation)	FEB 2018
552.232-78	Commercial Supplier Agreements Unenforceable Clauses	FEB 2018

I.4 DHS ACQUISITION REGULATION SUPPLEMENTS (HSAR) CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at HSAR website:

www.dhs.gov/publication/homeland-security-acquisition-regulation-deviations/

HSAR	TITLE	DATE
HSAR Class Deviation 15-01	Safeguarding of Sensitive Information	MAR 2015

I.5 OPTION FOR ADDITIONAL AS-NEEDED SERVICES

The Government may require additional, as-needed support during the base or any option period, and these modifications will be in-scope to provide increased support for the defined task areas of Section C. Additional, as-needed support is OPTIONAL and is not a guarantee. If the Government determines that an increased quantity of support is required for the task areas defined in Section C, the Government reserves the right to exercise the additional, as-needed support unilaterally. The CO will provide written notice to the Contractor at least 30 calendar days prior to any unilateral exercise of the additional, as-needed support services. In the event the Government does elect to exercise the additional, as-needed Option, support will be realigned under new or existing CLINs for the relevant task areas identified in Section C, and an equal amount will be deducted from the additional, as-needed support services CLIN amount. This support will be provided at the same labor rates that have been evaluated for cost realism and price reasonableness at time of TO award for the applicable ordering period.

J.1 LIST OF ATTACHMENTS

The following attachments are attached, either in full text or electronically at the end of the TO.

ATTACHMENT	TITLE
A	COR Appointment Letter
B	Acronym List
C	Incremental Funding Chart (electronically attached .xls)
D	Award Fee Determination Plan (AFDP)
E	Problem Notification Report (PNR) Template
F	Monthly Status Report (MSR) Template
G	Trip Report Template
H	Deliverable Acceptance-Rejection Report Template
I	Audit Readiness Assessment and Report Template
J	Department of Defense (DD) 254 (electronically attached .pdf)
K	Organizational Conflict of Interest (OCI) Statement
L	Corporate Non-Disclosure Agreement (NDA)
M	Travel Authorization Request (TAR) Template (electronically attached .xls)
N	Request to Initiate Purchase (RIP) Template (electronically attached .xls)
O	Consent to Purchase (CTP) Template (electronically attached .xls)
P	Sub-CLIN Detail
Q	ACOR Appointment Letters
R	Reserved
S	Key Personnel Qualification Matrix (KPQM)
T	Reserved
U	Acquisition Risk Questionnaire
V	Reserved
W	Reserved
X	Reserved